

Filed on behalf of Unified Patents, LLC
By: Jordan M. Rossen, Reg. No. 74,064
Ashraf Fawzy, Reg. No. 67,914
Unified Patents, LLC
4445 Willard Ave., Suite 600
Chevy Chase, MD, 20815
Email: jordan@unifiedpatents.com
afawzy@unifiedpatents.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, LLC
Petitioner

v.

DYNAPASS IP HOLDINGS LLC
Patent Owner

IPR2023-00425

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

TABLE OF CONTENTS

I. Introduction	1
II. Overview of Challenge and Relief Requested	1
A. Prior Art	1
B. Grounds for Challenge.....	1
C. U.S. 6,993,658	2
D. Prosecution History	4
E. Level of Ordinary Skill in the Art	5
F. Claim Construction.....	5
1. “a control module...configured to...”; “a communication module configured to...”; “an authentication module configured to...”	6
2. “Cell phone network”	9
3. “Not known to the user”	10
III. Grounds of Unpatentability.....	13
A. Ground 1: Claim 5 Is Obvious over <i>Veneklase</i> in view of <i>Jonsson</i>	13
1. Overview of <i>Veneklase</i>	13
2. Overview of <i>Jonsson</i>	15
3. Claim 5	17
Motivations to Combine <i>Veneklase</i> and <i>Jonsson</i>	31
B. Ground 2: Claims 1, 3-6 Are Obvious over <i>Kew</i> in view of <i>Sormunen</i>	46
1. Overview of <i>Kew</i>	46
2. Overview of <i>Sormunen</i>	49
3. Claim 5	50
Motivations to Combine <i>Kew</i> and <i>Sormunen</i>	58
4. Claim 6	71
5. Claim 1	72
6. Claim 3	75
7. Claim 4	77
C. Analogous Art.....	78
IV. Mandatory Notices	79
A. Real Party-in-Interest.....	79
B. Related Matters	79

C. Petitioner is aware that the '658 Patent has been challenged in IPR2023-00367 on January 3, 2022. Lead and Back-up Counsel	81
D. Service Information, Email, Hand Delivery, and Postal	81
V. Certification of Grounds for Standing	81
VI. Discretionary Institution	81
VII. Conclusion.....	85

TABLE OF EXHIBITS

Exhibit No.	Description
1001	U.S. Patent 6,993,658
1002	Prosecution History File of Application 09/519,829
1003	Declaration of Bruce McNair (¶¶1-168)
1004	Curriculum Vitae of Bruce McNair
1005	European Patent Application No. 084451 to Veneklasē (“ <i>Veneklasē</i> ”)
1006	PCT Patent Publication No. WO 96/00485 to Jonsson (“ <i>Jonsson</i> ”)
1007	PCT Patent Publication No. WO 95/19593 to Kew (“ <i>Kew</i> ”)
1008	PCT Patent Publication No. WO 97/31306 to Sormunen (“ <i>Sormunen</i> ”)
1009	Li Gong, “Optimal Authentication Protocols Resistant to Password Guessing Attacks,” Proceedings The Eighth IEEE Computer Security Foundations Workshop, 1995, pp. 24-29, doi: 10.1109/CSFW.1995.518549.
1010	U.S. Patent 3,938,091
1011	IETF RFC2289, “A One-Time Password System,” February 1989, available at https://www.rfc-editor.org/rfc/rfc2289.html

1012	U.S. Patent 5,276,444
1013	S.A. Sherman, R. Skibo, R.S. Murray, “Secure Network Access Using Multiple Applications of AT&T’s Smart Card,” AT&T Technical Journal, September/October 1994
1014	Lt. Gen. Charles R. Myers, “Vietnam Studies: Division-Level Communications, 1962-1973”, US Department of the Army, 1982, Ch. 8, retrieved from https://history.army.mil/catalog/pubs/90/90-11.html December 13, 2022.
1015	Z. J. Haas and S. Paul, "Limited-lifetime shared-access in mobile systems," Proceedings IEEE International Conference on Communications ICC '95, 1995, pp. 1404-1408 vol.3, doi: 10.1109/ICC.1995.524434
1016	Mobivity, A Brief History of Text Messaging, Sept. 27, 2012, available at https://www.mobivity.com/mobivity-blog/a-brief-history-of-text-messaging
1017	Declaration of Kevin Jakel (¶¶115)

I. INTRODUCTION

Unified Patents, LLC (“Petitioner” or “Unified”) respectfully submits this Petition for *Inter Partes* Review (“IPR”) of claims 1, 3-6 (“Challenged Claims”) of U.S. Patent 6,993,658 (“the ’658 Patent”) (EX1001).

II. OVERVIEW OF CHALLENGE AND RELIEF REQUESTED

A. Prior Art

The ’658 Patent was filed March 6, 2000.

Veneklase (EX1005) was filed October 22, 1997 and published May 27, 1998. Therefore, *Veneklase* qualifies as prior art under at least 35 U.S.C. §§ 102(a) and (b).

Jonsson (EX1006) was filed June 24, 1994 and published January 4, 1996. Therefore, *Jonsson* qualifies as prior art under at least 35 U.S.C. §§ 102(a) and (b).

Kew (EX1007) was filed January 12, 1995 and published July 20, 1995. Therefore, *Kew* qualifies as prior art under at least 35 U.S.C. §§ 102(a) and (b).

Sormunen (EX1008) was filed February 6, 1997 and published August 28, 1997. Therefore, *Sormunen* qualifies as prior art under at least 35 U.S.C. §§ 102(a) and (b).

B. Grounds for Challenge

Petitioner requests IPR under 35 U.S.C. § 311 of the Challenged Claims. They are unpatentable under 35 U.S.C. § 103.

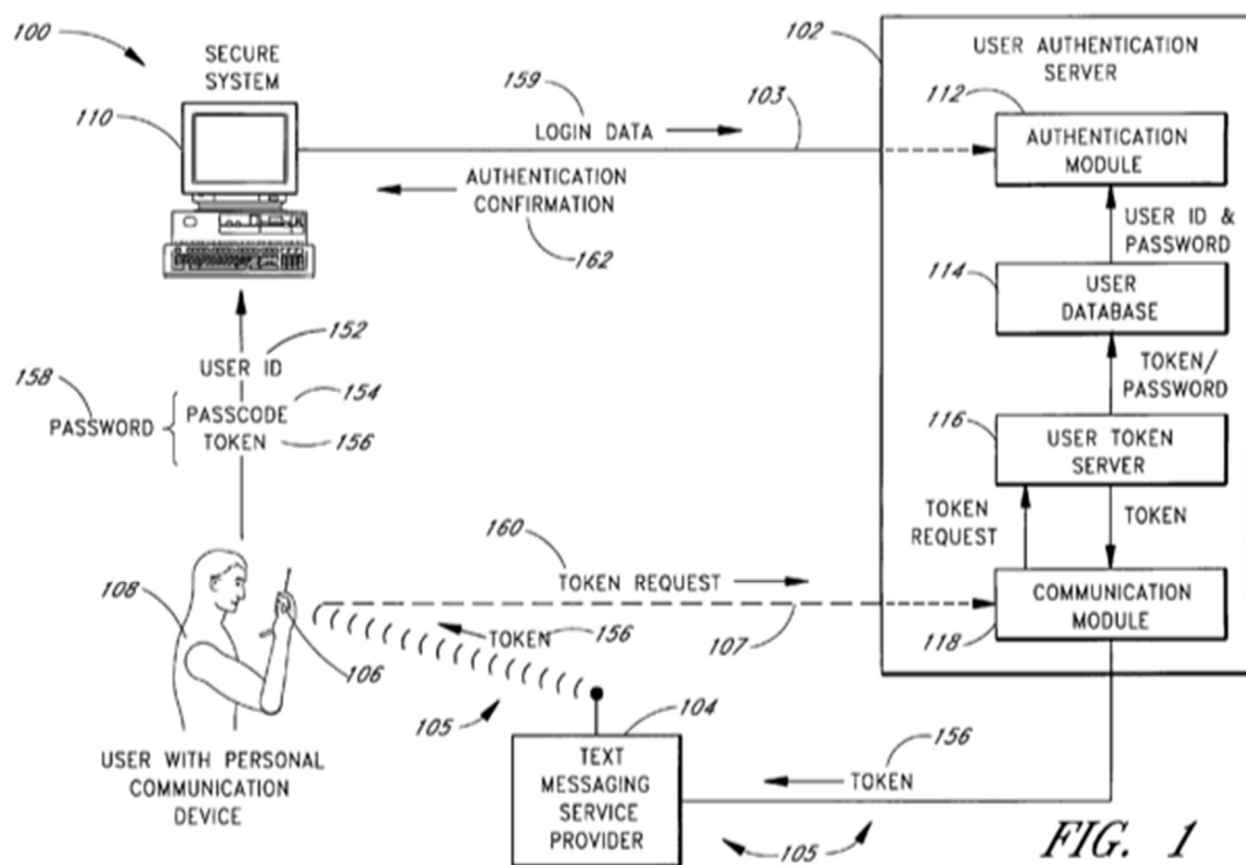
The grounds for challenge include:

Ground	References	Challenged Claims
1	<i>Veneklase</i> in view of <i>Jonsson</i>	5
2	<i>Kew</i> in view of <i>Sormunen</i>	1, 3-6

C. U.S. 6,993,658

The '658 Patent is directed to “the authentication of users of secure systems, and, more particularly, the invention relates to a system through which user tokens required for user authentication are supplied through personal communication devices such as mobile telephones and pagers.” EX1001, 1:7-11. Specifically, the '658 Patent describes an authentication system in which “access to the system is based upon: nonsecret information known to the user, such as the user ID; secret information known to the user, such as the passcode; and information provided to the user through an object possessed by the user, such as the token.” *Id.*, 2:11-15.

As shown in Figure 1, the '658 Patent teaches that “the user token server 116 generates a token,” and then creates the new password 158 based on the user’s passcode 154 and the newly generated token 156. *Id.*, 6:59-63.



Id., Fig. 1. “The token server 116 transmits the token 156 to the user’s personal communication device 106 via the token delivery communication link 105.” EX1001, 7:31-33. The ’658 Patent discloses that “[t]he communication module 118 forwards tokens 156 to a text messaging service provider 104, which may be a pager or mobile phone service provider,” which “then forwards the token 156...to the personal communication device 106.” *Id.*, 5:34-41.

After receiving the token, “the user 108 logs into the secure system 110 using the user ID 152 and the password 158,” where the password either “combines the passcode 154 and the token 152” or they are “submitted separately.” *Id.*, 7:40-45.

Once this information is entered into the system by the user, “the secure system 110 transmits login data 159 to the user authentication server 102 over the computer network 103 for authentication of the user 108” and “[i]n order to authenticate the user 108, the authentication server 102 preferably compares the login data to the password 158 (hashed or unhashed) or the passcode 154 and token 156 (hashed or unhashed) corresponding to the user ID 152 stored in the user database 114.” *Id.*, 7:46-63. Finally, “[i]f the token has an expiry time, the token 156 expires,” and “upon expiration of the token 156, the control module 402 deactivates the user account in the user database 114.” *Id.*, 9:60-64.

The '658 Patent has seven claims, including two independent claims. Claim 5 is the broadest claim and will thus be considered first. It is generally directed to an authentication system involving sending a token over a cell phone network and receiving a password based on the token and a passcode over a second network. EX1001, 12:12:20-49. Claim 1 is a method claim with similar elements, which also requires that the system receive a request via a token over the cell phone network. *Id.*, 11:43-12:13. EX1003, ¶¶52-59.

D. Prosecution History

The '658 Patent was filed on March 6, 2000. On March 11, 2004, Applicant responded to a rejection by arguing that Menezes could not meet the claimed element “generating a new password based at least upon a token and a passcode” and

“receiving the password from the user,” because Menezes’ system did not use a new token each time a login was requested and because the token was never sent to the user. EX1002, 109-124.

On May 12, 2005, Applicant responded to a final rejection by filing an RCE and heavily amending the claims to require additional elements, including a cell phone network, activation in response to the password, and deactivation within a predetermined amount of time. EX1002, 59-64.

On July 21, 2005, the Examiner issued a Notice of Allowance with an examiner’s amendment adding “a computer processor” and noting 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. EX1002, 45-49. EX1003, ¶¶60-62.

E. Level of Ordinary Skill in the Art

A POSITA for the ’658 Patent would have had at least (1) an undergraduate degree in electrical and computer engineering or a closely related field; and (2) two or more years of experience in security. EX1001, generally; EX1003, ¶¶49-51.

F. Claim Construction

In post-grant proceedings, claims are construed under the same standard as they would be construed by Article III courts. *See* 37 C.F.R. § 42.100(b). At this

time, Petitioner submits that the claims are obvious under any reasonable construction, but submits that all terms should be given their plain meaning. EX1003, ¶¶22-24. Petitioner addresses certain limitations below.

1. “a control module...configured to...”; “a communication module configured to...”; “an authentication module configured to...”

Some limitations recite a specific module that is “configured to” perform certain functions, such as create a new password based on certain factors, transmit a token, or receive a password and activate access to an account. Since “means” is not used, there is a rebuttable presumption against applying 35 U.S.C. § 112 ¶6 (“Paragraph 6”) to these limitations. *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1346 (Fed. Cir. 2015) (*en banc*). Given the absence of evidence showing that the claims lack sufficient structure, Paragraph 6 should not apply. *Dyfan, LLC v. Target Corp.*, 28 F.4th 1360 (Fed. Cir. 2022).

The Board may reach obviousness whether Paragraph 6 applies and even if the claims are indefinite. *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 801, 813-14 (Fed. Cir. 2021) (obviousness determination of indefinite means-plus-function claims possible, as indefiniteness precludes a patentability finding “only when the indefiniteness renders it logically impossible” to assess obviousness); *see also Huawei Techs. Co. v. WSOU Invs., LLC*, IPR2021-00226, Paper 10, 22 (P.T.A.B., June 10, 2021) (construction of potential means-plus-function terms unnecessary at

the institution stage).¹ And Paragraph 6 is inapplicable if the limitations have sufficient structure. Here, the claims recite algorithms that comprise receiving data, sending data, and storing data—all features of generic computers. *See In re Katz Interactive Call Processing Patent Litig.*, 639 F.3d 1303, 1316 (Fed. Cir. 2011) (algorithms unnecessary for functions like receiving, storing, and processing). In addition, the claimed modules “describe[] adequate structure for transmitting that motion data through conventional software and hardware.” *Blast Motion v. Zepp Labs*, 2017 WL 476428, *17 (Fed. Cir. 2017) (finding communications module not governed by 112(f)).

To the extent that it is determined that the module terms are means-plus-function, they should be given the following constructions:

a. “a control module...configured to”

The '658 Patent claims “a control module executed on the computer processor configured to” perform the following function: “create a new password based at least upon a token and a passcode” and “set a password associated with the user to be the

¹ Here, the prior art teachings are consistent with the specification’s disclosure for these claims, and the general public has an interest in the determination of patentability of the method claims, to which Paragraph 6 does not apply. Therefore, Petitioner requests IPR even if some claims are indefinite.

new password.” EX1001, 12:27-33. The specification provides the corresponding structure for the claimed function to be software executed on a “server” that performs the following algorithm: (1) associates user ID with passcode and phone number of user’s personal communication device, (2) generates a new password, and (3) sets or rests the password associated with the user ID. *See, e.g.*, EX1001, 2:32-48, 8:2-8, 8:53-9:44, Figs. 1, 4, 5; *see also WMS Gaming v. International Game Technology*, 184 F.3d 1339, 1349 (Fed. Cir. 1999). EX1003, ¶¶29-30.

b. “a communication module configured to”

The ’658 Patent claims “a communication module configured to” perform the following function: “transmit the token to the personal communication device through the cell phone network.” EX1001, 12:34-36. The specification provides the corresponding structure for the claimed function to be one of: (1) a mobile device with messaging capabilities, (2) a phone dialer, or (3) a connection card connected to a messaging service provider. *See, e.g.*, EX1001, 2:39-42, 5:66-6:1, 6:18-20, 10:14-41, Fig. 1. EX1003, ¶31.

c. “an authentication module configured to”

The ’658 Patent claims “an authentication module configured to” perform the following function: “receive the password from the user through a secure computer network” and “activate[] access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the

account.” EX1001, 12:37-45. The specification provides the corresponding structure for the claimed function to be software similar to that provided with operating systems executed on a “server” that performs the following algorithm: (1) receive a submitted password in response to a request for authentication and (2) grant access to the user if the submitted password matches the valid password. *See, e.g.*, EX001, 3:4-25, 5:3-10. Fig. 1. EX1003, ¶32.

2. “Cell phone network”

Claims 1 and 5 of the ’658 Patent require that the personal communication device communicates over a *cell phone network*. The ’658 Patent does not use the term cell phone network in the specification, but it does disclose that “[t]he communication module 118 forwards tokens 156 to a text messaging service provider 104, which may be **a pager or mobile phone service provider.**” EX1001, 5:32-40; *see also* 9:45-54, 4:13-17, 3:1-3, 2:28-31, 2:6-8, 1:7-11. Indeed, the ’658 Patent discloses an embodiment in which “the communication module 118 is a phone dialer 622, the personal communication device 106 is a pager 624, and the text messaging service provider is a paging service 626.” EX1001, 10:31-34. Furthermore, Claim 1 requires a personal communication device be in communication over a “cell phone network” and dependent claims 3 and 4 require that the personal communication device be a “mobile phone” and a “pager,” respectively. EX1001, 11:47-50, 12:16-19. Thus, a POSITA would have

understood that the *cell phone network*, as claimed by the '658 Patent, must at least include mobile device and pager service provider communication networks. EX1003, ¶25.

3. “Not known to the user”

Claims 1 and 5 of the '658 Patent require that the *token is not known to the user*. While the specification never explicitly discusses this limitation, it is clear from the embodiments disclosed in the '658 Patent that this term must mean “not known to the user before being sent to the user as part of the authentication process.” EX1003, ¶¶26-28. This is because the '658 Patent distinguishes between “secret information known to the user, such as the passcode” and “information provided to the user through an object possessed by the user, such as the token.” EX1005, 2:11-15. The '658 Patent further discloses that “token 156 is preferably provided only to the user 108 by the user authentication server 102 through the user’s personal communication device 106 on an as needed basis,” and in certain embodiments, “the user 108 combines the token 156 with the passcode 154 to form a password 158.” EX1005, 4:41-44, 4:52-53. Furthermore, the claims require the user to receive the token and input the password, which is based on the token and passcode. Therefore, a POSITA would have understood that the token would eventually need to be known to the user. EX1003, ¶¶26-28). Indeed, Figures 2A-D of the '658 Patent disclose “login screens that can be used in conjunction with various embodiments of the

invention,” and all three of the embodiments require the user to eventually be provided the token in order to input it into the computer, either by itself (e.g., Figs. B and C-D) or combined with the passcode (e.g., Fig. A). EX1005, Figs. 2A-D.

Logon To Network:

USER ID

PASSWORD

Note: Your password is your passcode followed by a valid token

FIG. 2A

Logon To Network:

USER ID

PASSCODE

TOKEN

FIG. 2B

Please enter a user ID to request a Token
Token will be instantly transmitted to your registered Personal
Communication Device and will be valid for one minute

USER ID

FIG. 2C

Logon To Network:

PASSCODE

TOKEN

FIG. 2D

Thus, a POSITA would have understood that *not known to the user*, as claimed by the '658 Patent, must include information that is not known to the user at the start of the process, but is eventually provided to the user. EX1003, ¶¶26-28.

III. GROUNDS OF UNPATENTABILITY

Pursuant to Rule 42.104(b)(4)-(5), the following sections (supported by Bruce McNair's Declaration, EX1003, ¶¶1-168) explain the grounds of unpatentability, the limitations of the Challenged Claims, and how these claims were obvious.

A. Ground 1: Claim 5 Is Obvious over *Veneklase* in view of *Jonsson*

1. Overview of *Veneklase*

Veneklase discloses a computer authentication system which is “adapted to grant an authorized individual access to a secured domain, such as a computer or data stream.” EX1005, Abstract. In particular, *Veneklase* discloses that a user contacts the host computer 402 and it “checks the received identification code and cross references the received password code against a pager phone number list resident within the user table 414.” EX1005, 8:1-5, Fig. 6.

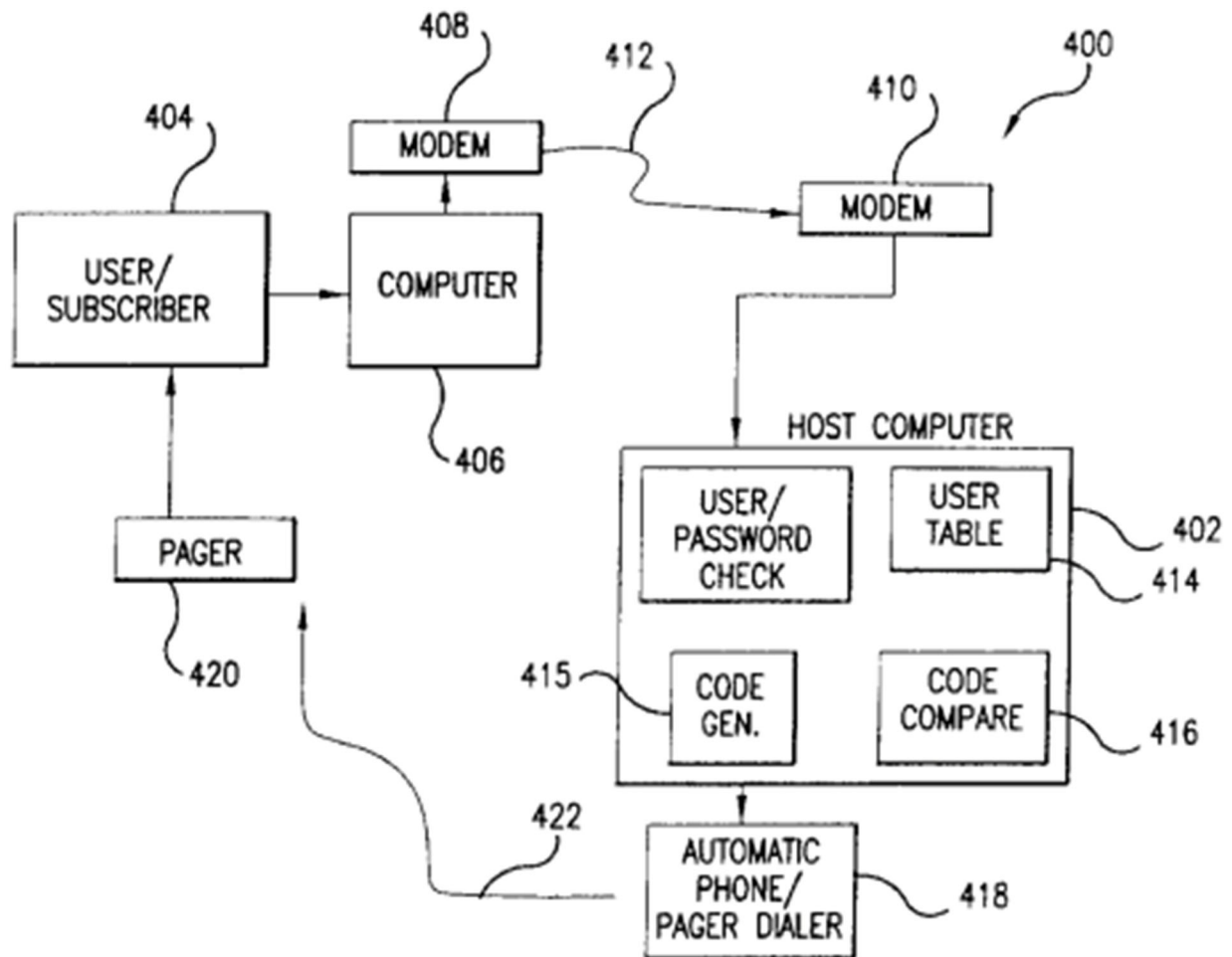


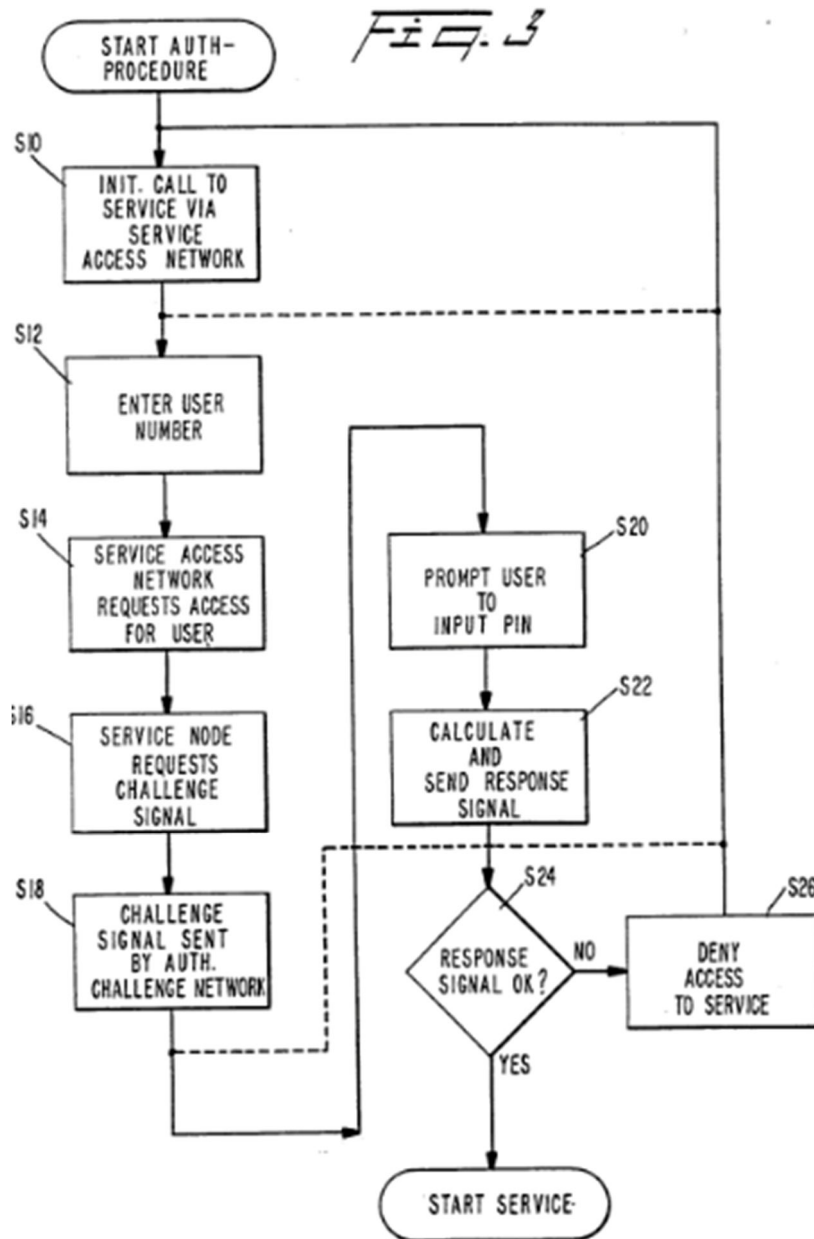
FIG. 6

If a match is made, it “causes the ‘code generator’ software subroutine 415 resident within computer 402, to generate a pseudo-random number code and passes the received code along with the authorized user’s pager number to the commercially available and conventional automatic dialer 41B,” which telephones a “pager 420 by means of conventional and commercially available communication channel 422 (e.g., voice line) and transmits the code to the user’s pager.” *Id.* 8:5-15. This communication and the initial sending of the random code to the personal device

“utilize[] two distinct communication channels.” EX1006, 7:11-28; *see also* 3:50-4:3. The user 404 “now enters the code he or she has received from the pager 420...and sends this password or pseudo-random code back to computer 402, where it is compared with the software subroutine module denoted as ‘code compare’ 416.” *Id.*, 8:18-24. “If the comparison yields a match, the user 404 is allowed access to computer 402 and/or a portion of computer 402.” *Id.*, 8:24-27. EX1003, ¶¶65-66.

2. Overview of *Jonsson*

Jonsson discloses a system for providing “[a]uthorization for a user to use a service” via “a modified pager which calculates a unique response code to a transmitted challenge code based on the challenge code, an input personal identification number, and an internal key.” EX1006, Abstract. As shown in Figure 3, “a user initiates communication to a service node 26 via the service access network 24,” e.g., by dialing an appropriate telephone number stored in their personal unit. EX1007, 10:13-18, Fig. 3.



In response to this request, the system “requests authentication via an authentication challenge network 28 by sending a challenge code...to the user’s personal unit 20.” *Id.*, 10:23-27. Then the user is prompted “to input, for example, a security code, such as a PIN,” and once entered, “the algorithm unit 21b of the personal unit 20 calculates and sends a response code...to the display.” *Id.*, 10:29-

33. *Jonsson* discloses that the algorithm “calculates a response code based on the received challenge code, the user input (e.g., PIN), and optionally the secret key.” EX1006, 8:12-14; *see also* 7:5-10, 9:23-25. Finally, the user “manually inputs the displayed response code to the terminal 22,” and it is transmitted via the service access network 24 to the service node 26, where “the authentication center 30 performs the comparison of the received response code to the expected response code.” *Id.*, 11:4-20. EX1003, ¶¶67-68.

3. Claim 5

[5.0] A user authentication system comprising

To the extent the preamble is deemed limiting,² *Veneklas* teaches it; any alleged differences would have been obvious. EX1003, ¶¶71-72. *Veneklas* discloses that “[s]everal embodiments of computer security systems are described and which are adapted to grant an authorized individual access to a secured domain, such as a computer or data stream.” EX1005, Abstract, Fig. 6.

² *Pacing Techs., LLC v. Garmin Intern., Inc.*, 778 F. 3d 1021, 1023–1024 (Fed. Cir. 2015) (preambles stating purpose or intended not normally limiting).

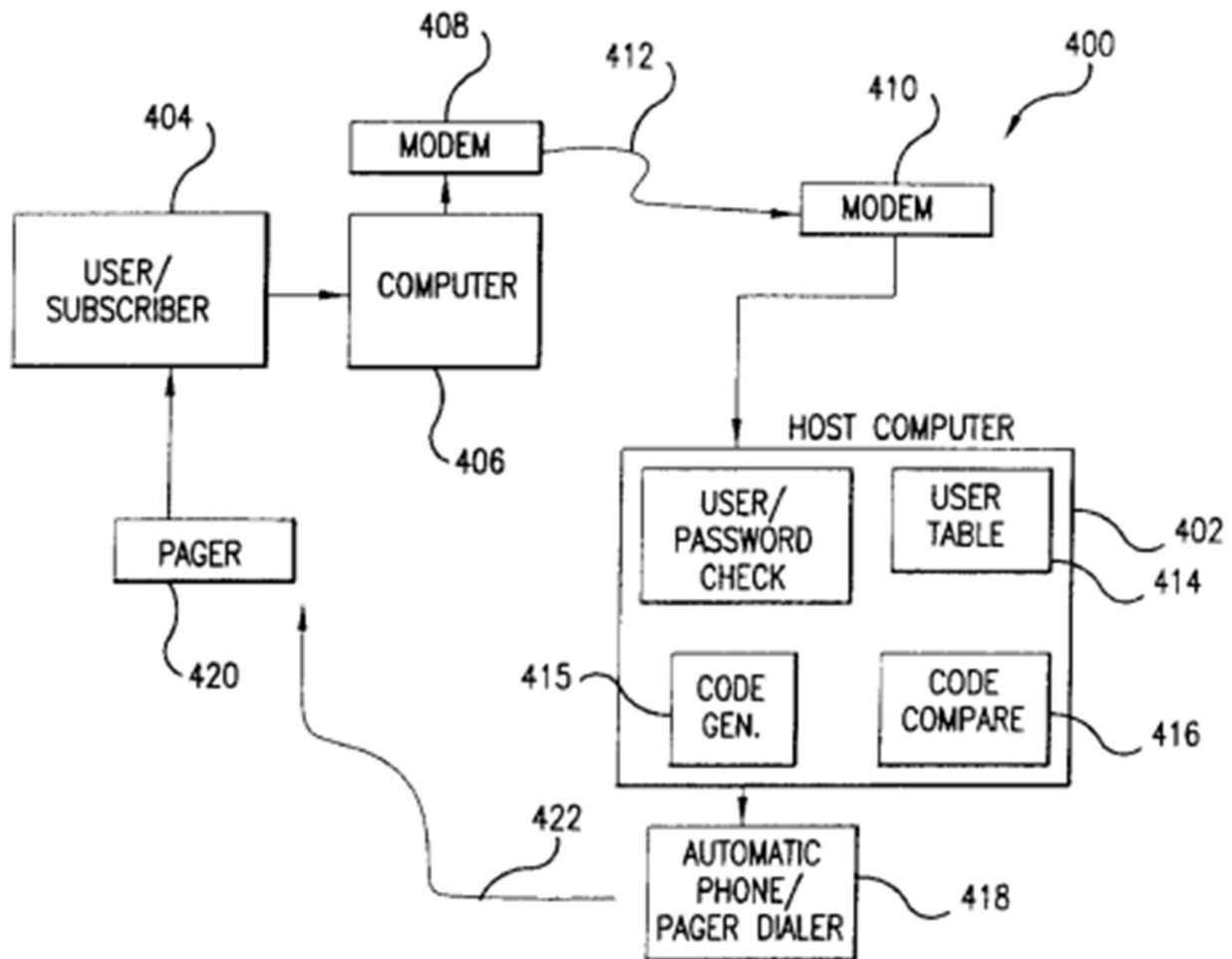


FIG. 6

Thus, *Venklase* teaches *user authentication system* (e.g., system adapted to grant an authorized individual access). EX1003, ¶¶71-72.

[5.1] a computer processor;

Venklase teaches this limitation; any alleged differences would have been obvious. EX1003, ¶¶73-76. Specifically, *Venklase* discloses that analyzing means 12 may comprise a **microprocessor and/or similar type of computer.**” EX1005, 5:35-37, Fig. 1.

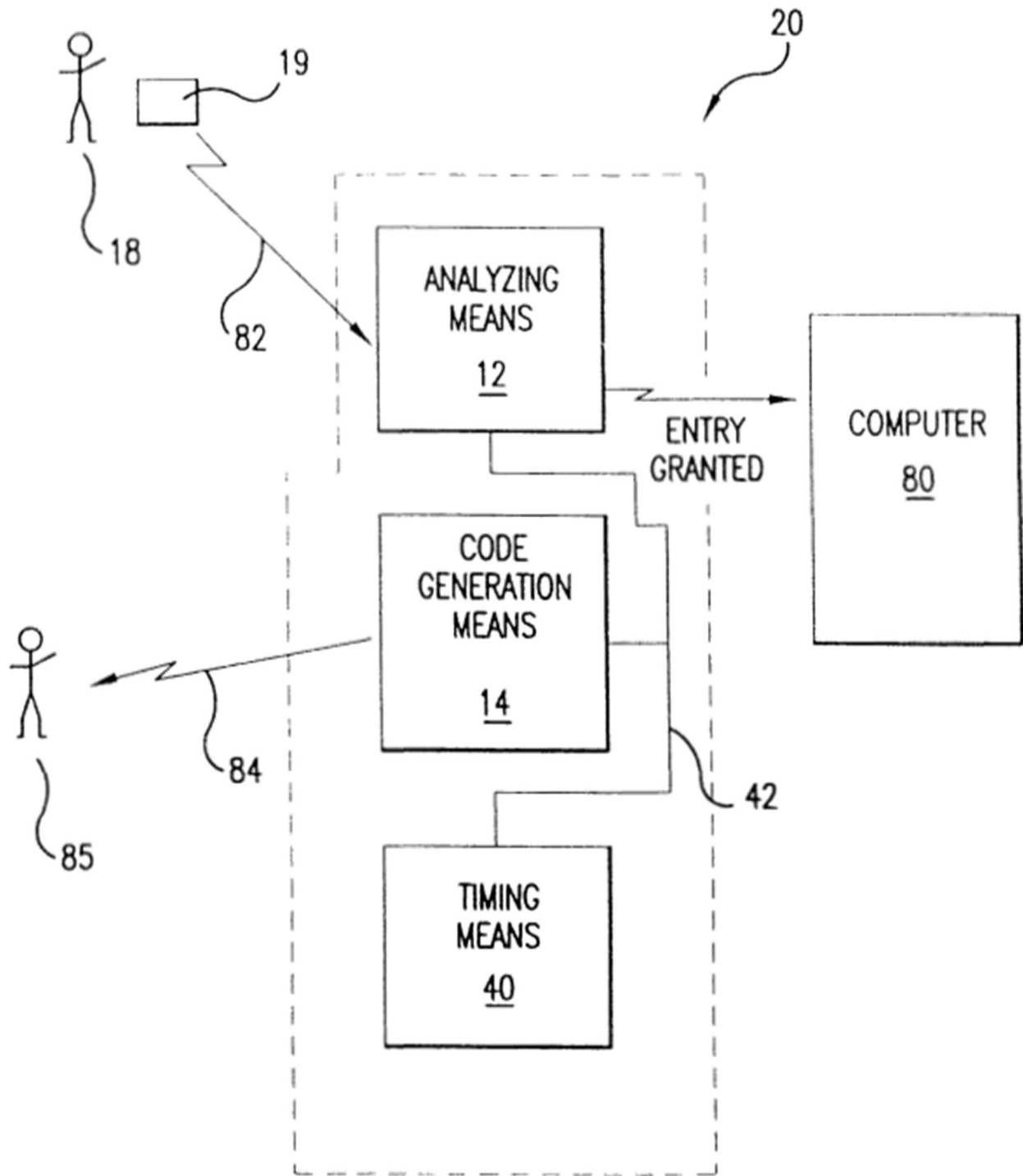
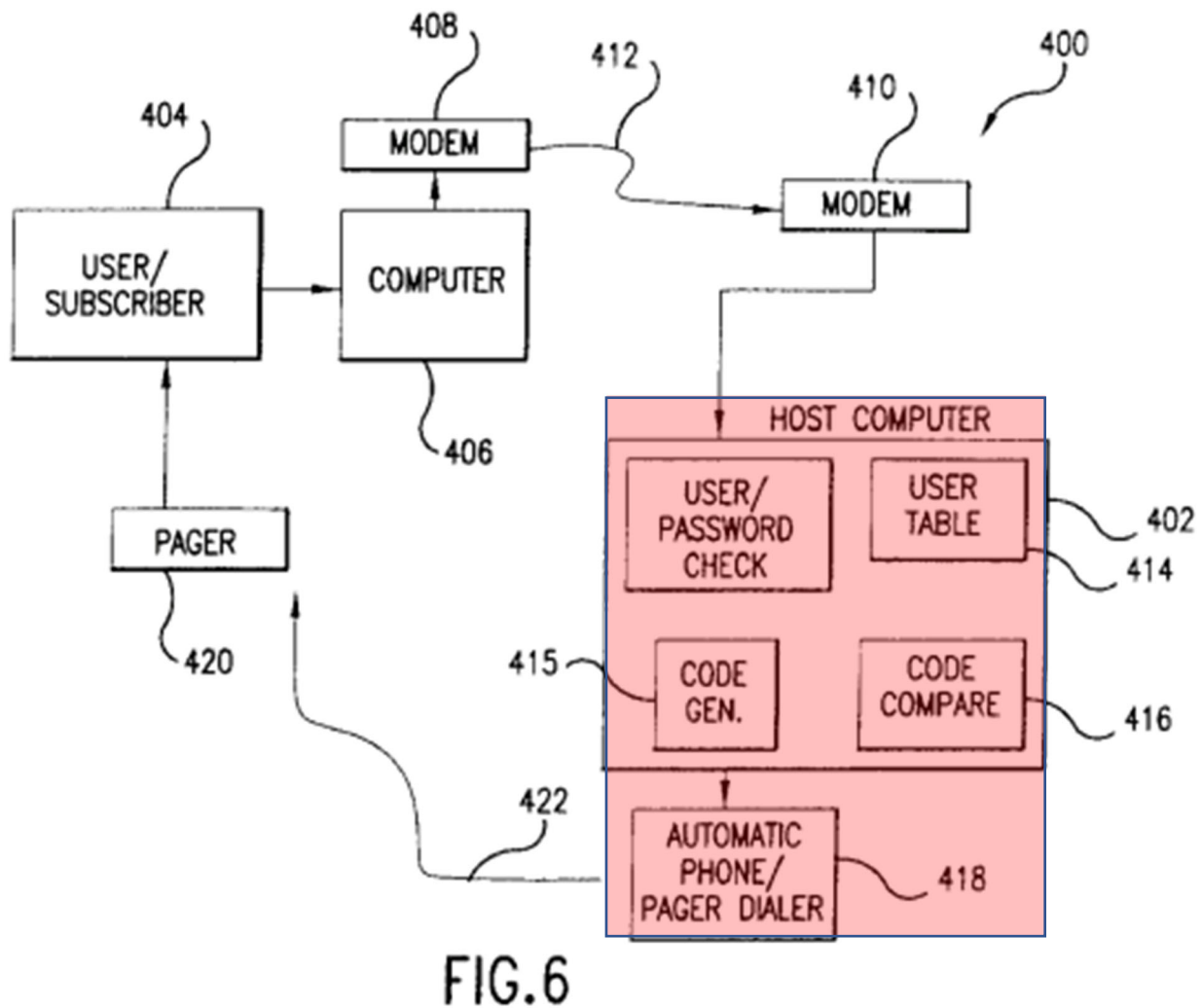


FIG. 1

Veneklase also discloses that the operations of its authentication system occur in host computer 402. See, e.g., EX1005, 7:29-8:27, Fig. 6.



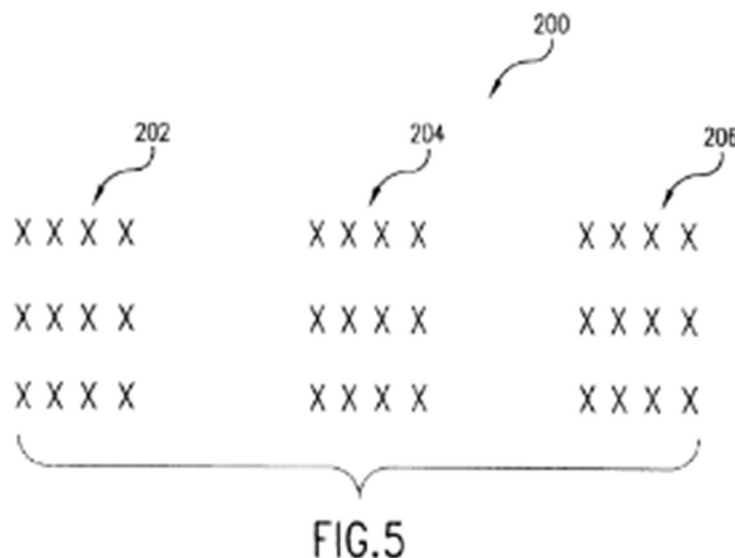
A POSITA would have understood that a computer capable of all of these actions, including checking codes against a database and generating random numbers would necessarily contain a computer processor. EX1003, ¶¶73-76.

Thus, *Veneklase* teaches a computer processor (e.g., microprocessor). *Id.*

[5.2] a user database configured to associate a user with a personal communication device possessed by the user, said

personal communication device configured to communicate over a cell phone network with the user authentication system;

Veneklase teaches this limitation; any alleged differences would have been obvious. EX1003, ¶¶77-82. *Veneklase* discloses that “**host computer 402 checks the received identification code and cross references the received password code against a pager phone number list resident within the user table 414** which is stored within computer 402.” EX1005, 8:1-5, Fig. 6; *see also* 6:15-26 (“each authorized password 202, contained in this master password list 200, has a unique first entry 204 associated with it and which **identifies the name of the authorized user who has been assigned that corresponding password and at least one telephone number 206 and/or network address associated with the identified user**”), Fig. 5 (showing the telephone number 206 associated with the user identification 204).



Furthermore, *Veneklase* discloses that the telephone number associated with the user identification is associated with a personal communication device, such as pager. EX1005, 8:1-5. This type of associating the user identification with a telephone number is exactly what is disclosed in the '658 Patent. *See, e.g.*, EX1001, 2:17-18 (“[t]he method includes associating a user ID with a phone number of a personal communication device”). Upon determining that the received identification code is matched with a pager phone number, “[t]he automatic dialer 418 telephones the conventional and commercially available pager 420 by means of **conventional and commercially available communication channel 422 (e.g. voice line).**” EX1005, 8:5-14.

Veneklase additionally teaches a *personal communication device configured to communicate over a cell phone network with the user authentication system*. For example, **communication channel 422** allows the **personal communication device** (e.g., **pager 420**) to communicate with the user **authentication system** (e.g., **host computer 402**, which includes automatic phone/pager dialer 418). *See, e.g.*, EX1005, Fig. 6.

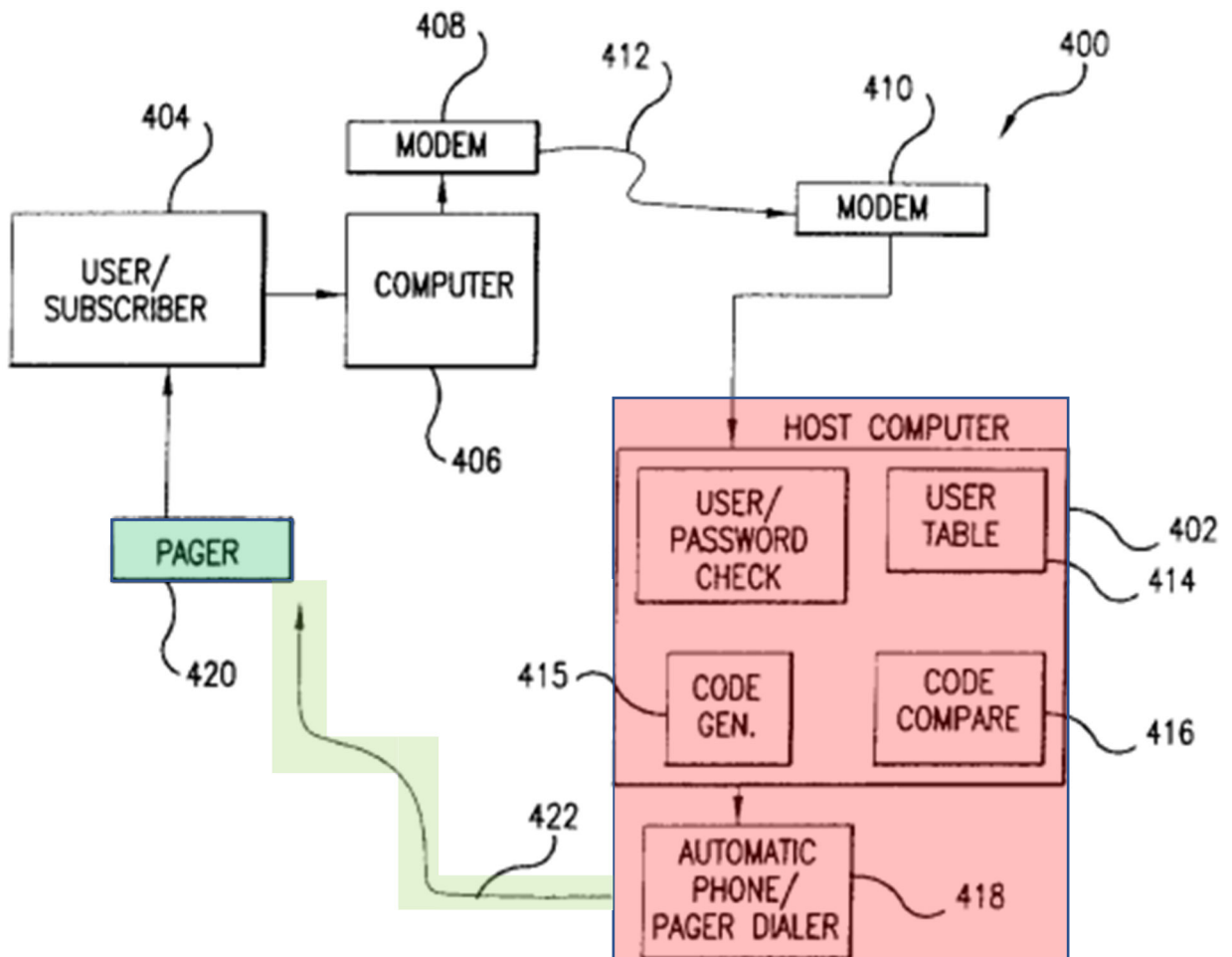


FIG.6

A POSITA would have understood that the “conventional and commercially available communication channel 422” described in *Veneklase* is the same type of cell phone network disclosed in the ’658 patent, which repeatedly makes clear that it covers both networks that communicate with cell phones and those that communicate with pagers. EX1003, ¶80. For instance, the ’658 Patent discloses that “[t]he communication module 118 forwards tokens 156 to a text messaging

service provider 104, which may be a pager or mobile phone service provider.” EX1001, 5:32-40; *see also* Abstract, 1:10-11, 2:6-8, 2:28-31, 3:1-3, 4:13-17, 9:45-54. Furthermore, *Veneklase* discloses that the communication channel over which the random code is sent could be a pager or a cell phone, stating that “the predetermined period of time would be shorter when **communications channel 84 comprises a pager or cellular phone**, since the owner has immediate access to the code upon transmission.” EX1005, 8:55-58. Thus, a POSITA would have understood that communication channel 422 meets the requirements of a *cell phone network* as claimed in the ’658 Patent, i.e., a mobile device or pager service provider communication network. EX1003, ¶¶77-80.

To the extent it is argued that the pager network disclosed in *Veneklase* does not satisfy the cell phone network limitation, a POSITA would have found it obvious to implement the authentication system of *Veneklase* using a cell phone network. EX1003, ¶81; *KSR Intern. Co. v. Teleflex Inc.*, 550 U.S. 398, 418-19 (2007). Indeed, *Veneklase* explicitly contemplates such a system, thus providing a teaching, suggestion, or motivation to modify it in such a way, as it notes that “the predetermined period of time would be shorter when **communications channel 84 comprises a pager or cellular phone**, since the owner has immediate access to the code upon transmission.” EX1005, 8:55-58. In addition, it would have been obvious to use a cell phone network to send *Veneklase*’s random code because doing so

would be a simple substitution of one known element for another and would have made the system available to even more users in more locations, which is one of the intentions of the reference. EX1003, ¶81. It would also have been obvious because it would have enabled users to use their cell phones to authenticate their access, which many users would prefer because they provide for larger screens and are thus easier to view. *Id.* A POSITA would have had a reasonable expectation of success in modifying *Veneklase*'s authentication system to use a cellular network instead of a pager network because they operate similarly, many times using the same protocols, and would just involve swapping out devices and making some software configuration changes. *Id.*

Thus, *Veneklase* teaches *a user database configured to associate a user with a personal communication device possessed by the user* (e.g., user table 414 that associates the name of the authorized user with at least one telephone number), *said personal communication device* (e.g., pager 420) *configured to communicate over a cell phone network* (e.g., communication channel 422) *with the user authentication system* (e.g., host computer 402). EX1003, ¶¶77-82.

[5.3] a control module executed on the computer processor configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the

control module further configured to set a password associated with the user to be the new password;

Veneklase in combination with *Jonsson* teaches this limitation; any alleged differences would have been obvious. EX1003, ¶¶83-90. *Veneklase* discloses “the steps of assigning a password to the user; receiving the password by use of a first communication channel; generating a code in response to the received password; transmitting the code by use of a second communications channel to the user; transmitting the code to the computer; and allowing access to the computer only after the code is transmitted to the computer.” EX1005, 4:8-15.

Veneklase discloses a **user/password check module** (i.e., a **control module**) located on the **host computer system 402** (i.e., the computer processor), as shown below in Figure 6. EX1005, Fig. 6.

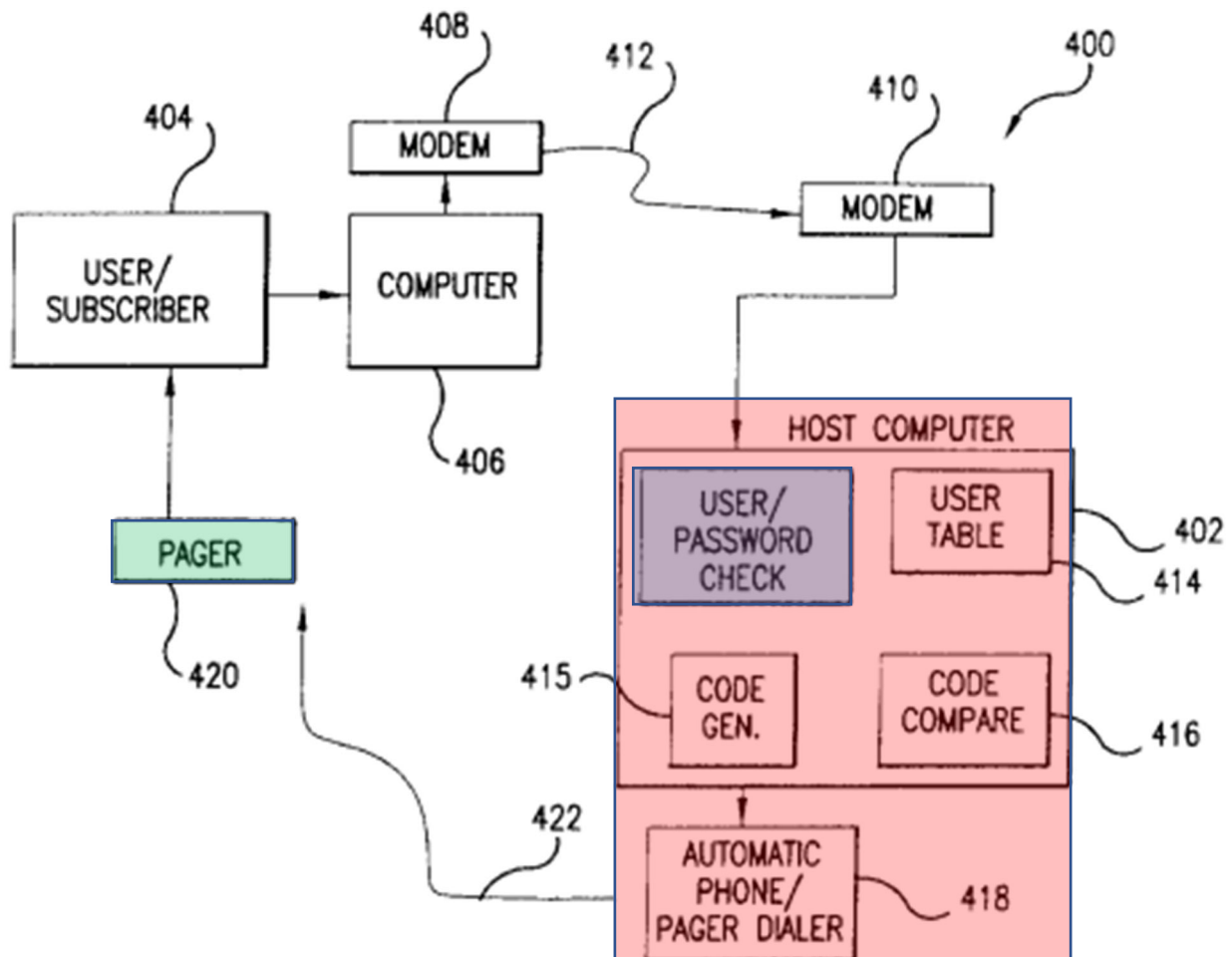


FIG.6

This user/password check module assigns two passwords, one that is known to the user and one that is not previously known to the user. It assigns a password that is previously known to the user, by virtue of it being a “received password” that is received from the user via the computer and then “generate[s] a substantially random and/or pseudo-random number or code,” which is sent to the user on their mobile device and then input into the computer by the user. *See, e.g.,* EX1004, 3:3-10. The random code meets the construction of not known to the user by virtue of

it being unknown to the user until it is received by the user via their personal device, which is how the '658 Patent itself discloses it, as explained in the claim construction section. EX1003, ¶¶83-85, 25.

While *Veneklase* teaches an authentication system in which the user inputs both a token that is not known to the user beforehand (e.g., the random code) and a passcode that is known to the user (e.g., the received password), it does not disclose creating a new password based on those two items. However, it would have been obvious to combine those two steps and instead create a new password based on both of them. For instance, *Jonsson* discloses a similar authentication system *configured to create a new password* (e.g., response code) *based at least upon a token* (e.g., challenge code) *and a passcode* (e.g., input security number), *wherein the token is not known to the user* (e.g., generated by the system) *and wherein the passcode is known to the user* (e.g., input by the user), *the control module further configured to set a password associated with the user to be the new password* (e.g., using the response code as the comparison).

Specifically, *Jonsson* discloses that the system includes a service node that “generates a challenge code and requests that the challenge code be sent to the personal unit 20 via an authentication challenge network 28.” EX1006, 4:24-5:6. This challenge code generated by the system is a *token* because it is not known to the user before it is generated and sent to the user. EX1003, ¶¶86-87. In addition,

Jonsson discloses the use of a “user input such as a personal identification number (PIN),” which by its very nature of being a user defined input, is known to the user beforehand. EX1006, 3:3-10. Indeed, *Jonsson* discloses that the challenge code is “unique for each transaction” and “the PIN or other user input may be changed from time to time.” EX1006, 3:14-18; *see also* 7:32-8:11 (“the user input, such as a PIN, can be updated at the user’s discretion or on a regular basis”).

Jonsson discloses an algorithm that **“calculates a response code [e.g., new password] based on the received challenge code [e.g., token], the user input (e.g., PIN) [e.g., passcode], and optionally the secret key.”** EX1006, 8:12-14; *see also* 7:5-10, 9:23-25. “Thus, for a correct response code to be generated, the challenge code, the user input and the secret key (if used) have to be in accordance with the expectations of the service node 26 or authentication center 30 if access to the service is to be granted.” *Id.*, 8:14-18. *Jonsson* further discloses that “[t]his provides a triple check on the identity of the user, requiring information from three separate sources (user: PIN, service node or authentication center: challenge code, and provider of the personal unit: secret key, thereby increasing the relative security of the transaction against fraud or other unauthorized use. EX1006, 7:18-23. Finally, *Jonsson* discloses *set[ting] a password associated with the user to be the new password*. Specifically, *Jonsson* discloses that “[t]he response code is compared to an **expected response code [e.g., a created new password], which, in**

exemplary embodiments, may be pre-stored [e.g., set as the new password] or generated using the same algorithm and variables.” EX1006, 10:2-5. A POSITA would have understood that this pre-stored expected response code is a new password associated with the user. EX1003, ¶88. The response code is a new password because *Jonsson* discloses that “[t]he response code is to be **unique to each transaction.**” EX1006, 7:34-35; *see also* EX1002, 121 (Applicant traversing prior art for not having a response code that is unique to each transaction).

In combination, *Veneklase*’s authentication system would incorporate *Jonsson*’s teachings related to using an algorithm to create a new password (e.g., response code) based on a known passcode (e.g., the received password/PIN) and an unknown token (e.g., the random code/challenge code). EX1003, ¶¶83-89.

Thus, *Veneklase* in combination with *Jonsson* teaches *a control module* (e.g., user/password check module) *executed on the computer processor configured to create a new password* (e.g., assigning a password to the user) *based at least upon a token* (e.g., random code) *and a passcode* (e.g., received password), *wherein the token is not known to the user* (e.g., generated by the system) *and wherein the passcode is known to the user* (e.g., received from the user), *the control module further configured to set a password associated with the user to be the new password* (e.g., set an expected response code). EX1003, ¶¶83-90.

Motivations to Combine *Veneklase* and *Jonsson*

It would have been obvious to incorporate *Jonsson*'s teachings related to an authentication system in which a password is created based on known and unknown inputs into *Veneklase*'s authentication system that utilizes both a known password and an unknown random code as of March 6, 2000. EX1003, ¶¶91-96. *Veneklase* teaches a system which a user inputs a password known beforehand, receives a randomly generated previously-unknown code, and then inputs that for authentication purposes. *See, e.g.*, EX1005, 7:52-8:27. *Jonsson* discloses a similar authentication system that involves the user inputting both a known PIN and a previously-unknown generated challenge code. *See, e.g.*, EX1006, 10:22-31. *Jonsson* discloses an algorithm that “calculates a response code based on the received challenge code, [and] the user input (e.g., PIN).” EX1006, 8:12-14. A POSITA would have been motivated to make such a combination because having only the one password transmitted via the computer system is more efficient and secure. EX1003, ¶91. *Veneklase*'s system allows for authentication through user input of a known and unknown code at separate times in a two-step process, while a POSITA would look to *Jonsson* because it would provide the added benefit of reducing the steps to a single step and thus reducing the amount of time required for the authentication process. *Id.* Furthermore, a POSITA would have been motivated to make such a combination because implementing *Veneklase*'s authentication

system with the algorithm of *Jonsson*'s system provides an additional layer of security. A POSITA would have understood that the algorithm system has the added security benefit of preventing unauthorized personnel from being able to access the system by engaging in SIM swapping. SIM swapping is a well-known trick of hackers in which they contact your service provider and activate a new SIM card on a different device in order to receive the user's authentication token. Doing so would not work in the combined system, because they would need access to the device containing the correct algorithm. EX1006, 2:43-45. EX1003, ¶91.

Furthermore, *Veneklase* explicitly provides a teaching, suggestion, and motivation for combining it with an authentication system that uses an algorithm, such as taught in *Jonsson*, because it explicitly discloses embodiments in which data streams are encoded and decoded using algorithms for additional security. *See, e.g.*, EX1005, 9:26-10:11; *KSR*, 550 U.S. at 418-19. Thus, a POSITA would have been motivated to use an algorithm for creating a new password based on the known password and the previously-unknown randomly generated code, such as described in *Jonsson*, to provide additional security. EX1003, ¶92.

It should be noted that while *Veneklase* mentions certain weaknesses related to certain specific uses of encryption algorithms in the background section, this is in the context of “modifying and/or changing the transmitted data in a certain manner, and/or requiring the transmission and receipt of modified data before access is

granted.” EX1005, 2:37-56. These drawbacks would not apply in the context of the algorithm for creating a new password disclosed in *Jonsson*, because it does not “provide[] all of the transmitted data, in some form.” *Id.*; EX1003, ¶93. In other words, the drawbacks noted in *Veneklase* are directed to encrypting all of the data as compared to using encryption to create a new password to access the data. Additionally, the combination would still utilize all of the protections provided for in *Veneklase*, so it only provides additional security (not less). *Id.* Finally, *Jonsson* clearly discloses that “[t]he specific algorithm used in a given embodiment is not germane to the present invention” and “[a]lgorithms of this type are known in the art or readily derived therefrom” (EX1006, 7:10-14), so a POSITA would not have been concerned about the cost or complexity of such algorithms. EX1003, ¶93. In addition, the Federal Circuit has stated that “[a] reference that merely expresses a general preference for an alternative invention but does not criticize, discredit, or otherwise discourage investigation into the claimed invention does not teach away.” *Meiresonne v. Google, Inc.*, 849 F.3d 1379, 1382 (Fed. Cir. 2017) (internal citations omitted).

A POSITA would further be motivated to combine *Veneklase* and *Jonsson* because the combination merely uses a known technique to improve similar devices in the same way. *See KSR*, 550 U.S. at 401. For instance, a POSITA would have been motivated to utilize the algorithm of *Jonsson* in the system of *Veneklase*

because it would have been used in the same way, i.e., to provide another layer of security. EX1006, 7:5-17. As discussed above, *Veneklase* discloses the use of known passwords and previously unknown randomly generated codes, so it would have been obvious for a POSITA to combine the two inputs. EX1003, ¶¶94.

A POSITA would have had a reasonable expectation of success in modifying *Veneklase*'s authentication system, which requires the use of both a known password and a previously-unknown randomly generated code, to create a new password based on those two values, as taught by *Jonsson*, because doing so would have merely made two steps into one without requiring any additional hardware. EX1003, ¶¶95.

Therefore, a POSITA would have been motivated to combine, and would have had a reasonable expectation of success in combining, *Veneklase*'s teachings, including a control module executed on the computer processor configured to create a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user with *Jonsson*'s teaching related to creating a new password based at least upon the token and setting that new password to be the new password. EX1003, ¶¶91-96. Thus, *Veneklase*, in combination with *Jonsson*, teaches this limitation.

[5.4] a communication module configured to transmit the token to the personal communication device through the cell phone network, and

Veneklase teaches this limitation; any alleged differences would have been obvious. EX1003, ¶¶97-100. *Veneklase* discloses *a communication module (e.g., automatic phone/pager dialer 418) configured to transmit the token to the personal communication device through the cell phone network (e.g., transmit the random code through communication channel 422)*. Specifically, *Veneklase* discloses that “host computer 402 checks the received identification code and cross references the received password code against a pager phone number list resident within the user table 414 which is stored within computer 402.” Then, the generated random number code and pager number are passed “to the **commercially available and conventional automatic dialer 418**,” which “**telephones the conventional and commercially available pager 420 by means of conventional and commercially available communication channel 422 (e.g., voice line) and transmits the code to the user’s pager.**” EX1006, 7:52-8:17, Fig. 6.

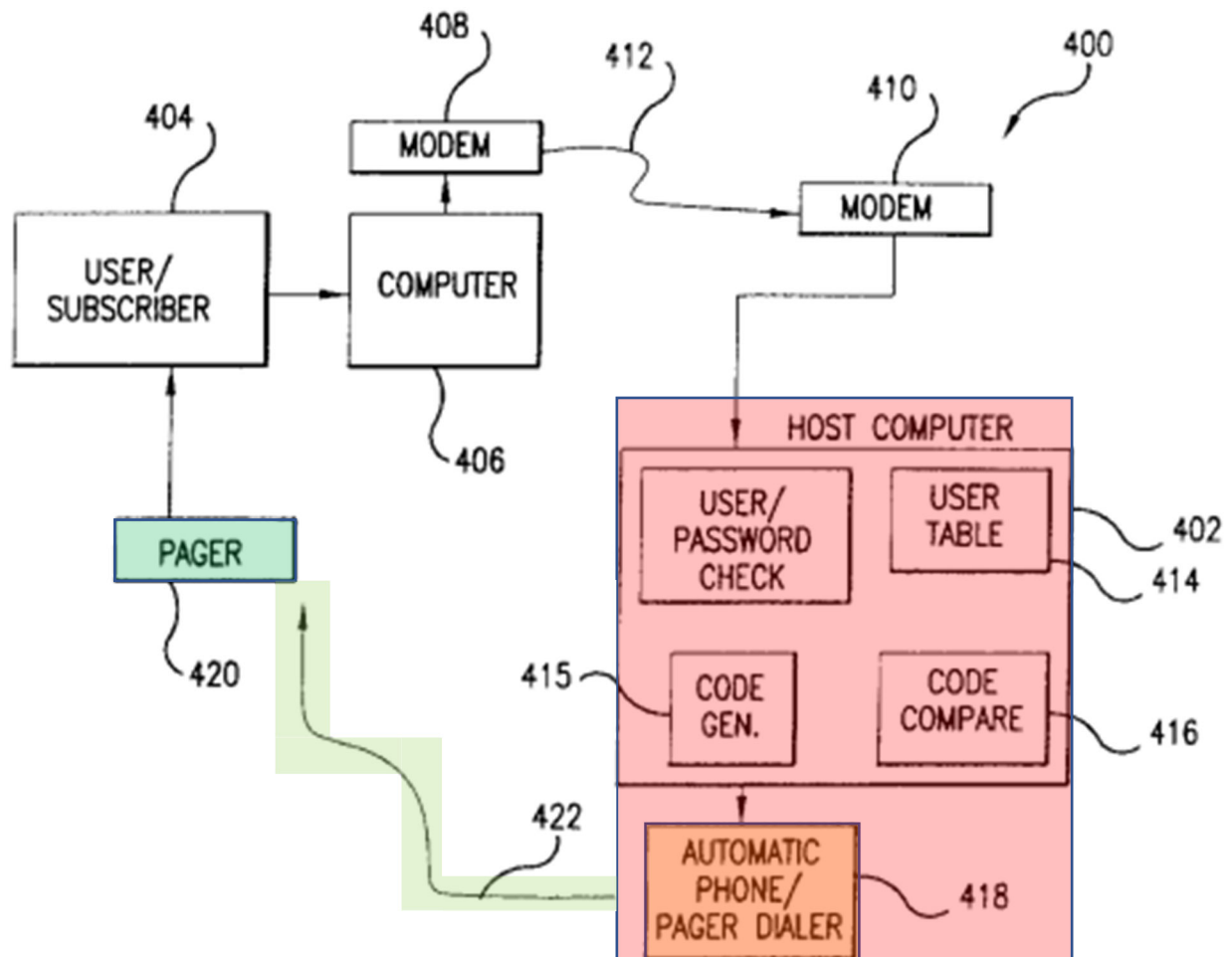


FIG. 6

A POSITA would have understood that the “conventional and commercially available communication channel 422” described in *Veneklase* is the same type of cell phone network disclosed in the ’658 patent, which repeatedly makes clear that it covers both networks that communicate with cell phones and those that communicate with pagers. EX1003, ¶¶97-99. For instance, the ’658 Patent discloses that “[t]he communication module 118 forwards tokens 156 to a text messaging service provider 104, which may be a pager or mobile phone service provider.”

EX1001, 5:32-40; *see also* Abstract, 1:10-11, 2:6-8, 2:28-31, 3:1-3, 4:13-17, 9:45-54. Furthermore, *Veneklase* discloses that the communication channel over which the random code is sent could be a pager or a cell phone, stating that “the predetermined period of time would be shorter when **communications channel 84 comprises a pager or cellular phone**, since the owner has immediate access to the code upon transmission.” EX1005, 8:55-58. Thus, a POSITA would have understood that communication channel 422 meets the requirements of a *cell phone network* as claimed in the ’658 Patent, i.e., a mobile device or pager service provider communication network. EX1003, ¶¶97-100.

Furthermore, the ’658 Patent discloses an embodiment in which “the **communication module 118 is a phone dialer 622, the personal communication device 106 is a pager 624, and the text messaging service provider is a paging service 626.**” EX1001, 10:31-34. This is very similar to what is disclosed in *Veneklase*. Thus, it is clear that the “cell phone network” claimed in the ’658 Patent also includes a pager network, as disclosed in *Veneklase*. EX1003, ¶¶97-100.

Thus, *Veneklase* teaches a *communication module* (e.g., automatic phone/pager dialer 418) *configured to transmit the token to the personal communication device through the cell phone network* (e.g., transmit the random code through communication channel 422). *Id.*

[5.5] an authentication module configured to receive the password from the user through a secure computer network, said secure computer network being different from the cell phone network,

Veneklase, alone or in combination with *Jonsson*, teaches this limitation; any alleged differences would have been obvious. EX1003, ¶¶101-105. *Veneklase* discloses *an authentication module* (e.g., code compare module 416) *configured to receive the password from the user through a secure computer network* (e.g., by receiving the random code via a typical communication channel 412). Specifically, *Veneklase* discloses that “user 404 now enters the code he or she has received from the pager 420...and **sends this password or pseudo-random code back to computer 402 where it is compared within the software subroutine module denoted as ‘code compare’ 416.**” EX1006, 8:18-27; *see also* 3:50-4:3. *Veneklase* discloses that its system will “allow that individual access to the computer system only if that individual generates and communicates the code to the code generation means.” *Id.*

In the combination with *Jonsson* discussed with respect to element [5.3], a POSITA would have understood that the new password (e.g., response code) being sent back to computer 402 and compared against the expected value is the one created by the algorithm based on both the known passcode (e.g., PIN) and the randomly generated token (e.g., challenge code). EX1003, ¶¶102, 83-89.

Veneklase further discloses *said secure computer network* (e.g., typical communication channel 412) *being different from the cell phone network* (e.g., a distinct communication channel different from communication channel 422). Specifically, *Veneklase* discloses that this communication in which the user submits its credentials to the host computer and the initial sending of the random code to the personal device “**utilize[] two distinct communication channels.**” EX1005, 7:11-28; *see also* 3:50-4:3. *Veneklase* discloses that “individual 404, in this implementation example, utilizes a commercially available and conventional computer 406 and a commercially available and conventional modem 408 to communicate with a commercially available and conventional modem 410 by means of a **typical communications channel (e.g. a conventional ‘dial-up’ telephone line) 412.**” *Id.*, 7:29-51. This is distinct from the “**conventional and commercially available communication channel 422** (e.g., voice line) [that] transmits the code to the user’s pager.” *Id.*, 8:11-17; *see also* Fig. 6 (showing distinct communication networks 412 and 422).

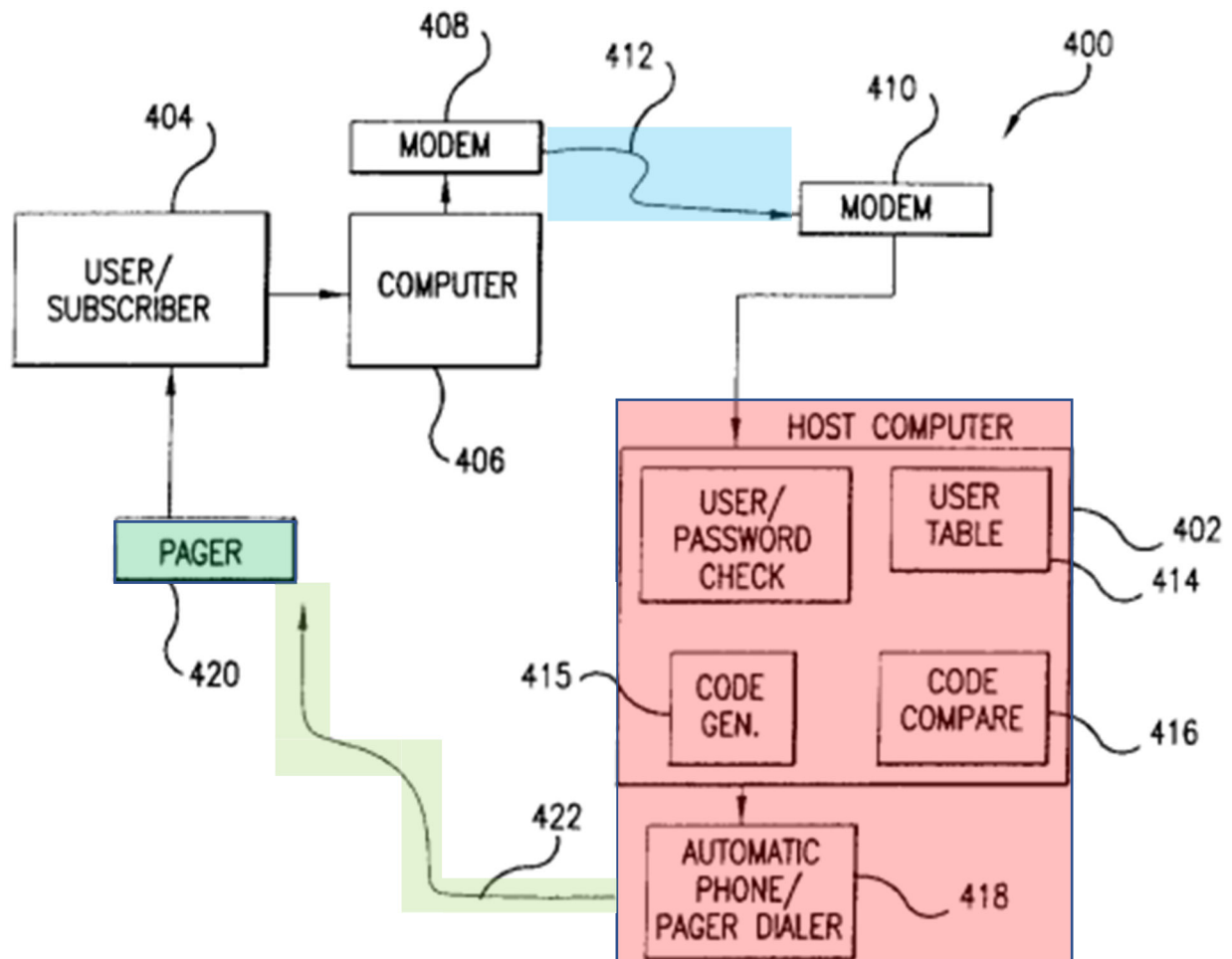


FIG. 6

A POSITA would have understood that this communication network is *secure computer network* because the use of the authentication procedures described in *Veneklase* make secure the host computer system. *See, e.g.*, EX1005, 9:3-14 (describing the host computer system as “the secured domain”); EX1003, ¶¶101-104. This is similar to what the ’465 Patent describes, which is “for a secure system, such as a computer system.” EX1001, 1:63-65; *see also* 2:49-3:3; 4:9-26.

Thus, *Veneklase*, alone or in combination with *Jonsson*, teaches an authentication module (e.g., code compare module 416) configured to receive the password from the user through a secure computer network (e.g., by receiving the password via a typical communication channel 412), said secure computer network being different from the cell phone network (e.g., a distinct communication channel different from communication channel 422). EX1003, ¶¶101-105.

[5.6] wherein the user has an account on the secure computer network, wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account, such that said account is not accessible through any password via the secure computer network.

Veneklase, in combination with *Jonsson*, teaches this limitation; any alleged differences would have been obvious. EX1003, ¶¶106-111. *Veneklase* discloses wherein the authentication module (e.g., code compare module 416) activates access to the account in response to the password (e.g., allows access if the random codes match). Specifically, *Veneklase* discloses that the user 404 “sends this password or pseudo-random code back to computer 402 where it is **compared within the software subroutine module denoted as ‘code compare’ 416** in Figure 6” and “[i]f the comparison yields a match, the user 404 is allowed access to computer 402 and/or to a portion of computer 402.” EX1006, 8:18-27; see also 6:45-7:10.

In addition, *Veneklase* discloses *wherein the user has an account on the secure computer network* (e.g., the user's password is found on the master password list). Specifically, *Veneklase* discloses that this system is implemented only when the password is found within the master password list. EX1005, 6:15-26 (“each authorized password 202, contained in this master password list 200, has a unique first entry 204 associated with it and which identifies the name of the authorized user who has been assigned that corresponding password and at least one telephone number 206 and/or network address associated with the identified user”). Thus, a POSITA would have understood that in order for the password associated with the authorized user to appear in the list, that user needs to have an account on the secure computer network. EX1003, ¶¶106-107.

Veneklase also discloses that its system *deactivates the account within a predetermined amount of time after activating the account* (e.g., denies entry if not received in the predetermined time window), *such that said account is not accessible through any password via the secure computer network* (e.g., not accessible without the random code). Specifically, *Veneklase* discloses an embodiment which “includes a timer or ‘timing means’ 40 which may comprise one or more software subroutines which are adapted to operate and/or execute within and/or upon computer 80,” such as a watchdog timer. EX1006, 8:28-39. *Veneklase* discloses that “timing means 40 records the time at which the first and second passwords are

received by analyzing means 12” and “then compares the times to determine whether the second password was received **within a predetermined period** or predetermined ‘window’ of time after the first password was received.” EX1005, 8:40-49. “If the second password was not received within the predetermined period of time, analyzing means 12 denies entry to the secured domain (e.g., computer 80).” *Id.*, 9:3-6. A POSITA would have understood that this is true no matter whether the user has the correct password, and thus *said account is not accessible through any password via the secure computer network*. EX1003, ¶108.

In the combination with *Jonsson* discussed with respect to element [5.3], a POSITA would have understood that the new password (e.g., response code) being sent back to computer 402 and compared against the expected value is the one created by the algorithm based on both the known passcode (e.g., PIN) and the randomly generated token (e.g., challenge code). EX1003, ¶¶19, 83-89. Thus, the predetermined period would be the time between the receipt of the token (e.g., randomly generated challenge code) and the sending back of the newly created password (e.g., response code). *Id.*

Veneklase’s teaching is within the scope of the recited deactivating limitation because it is nearly identical to how this limitation is described in the ’658 Patent. Indeed, the ’658 Patent discloses in Figure 5 that the “user can access secure system by logging in using token” in step 516, but if the “token expires” in step 518, it

“deactivate[s] user account in user database.” EX1001, Fig. 5; 9:61-64 (“At a step 518, if the token has an expiry time, the token 156 expires. At a step 520, upon expiration of the token 156, the control module 402 deactivates the user account in the user database 114.”).

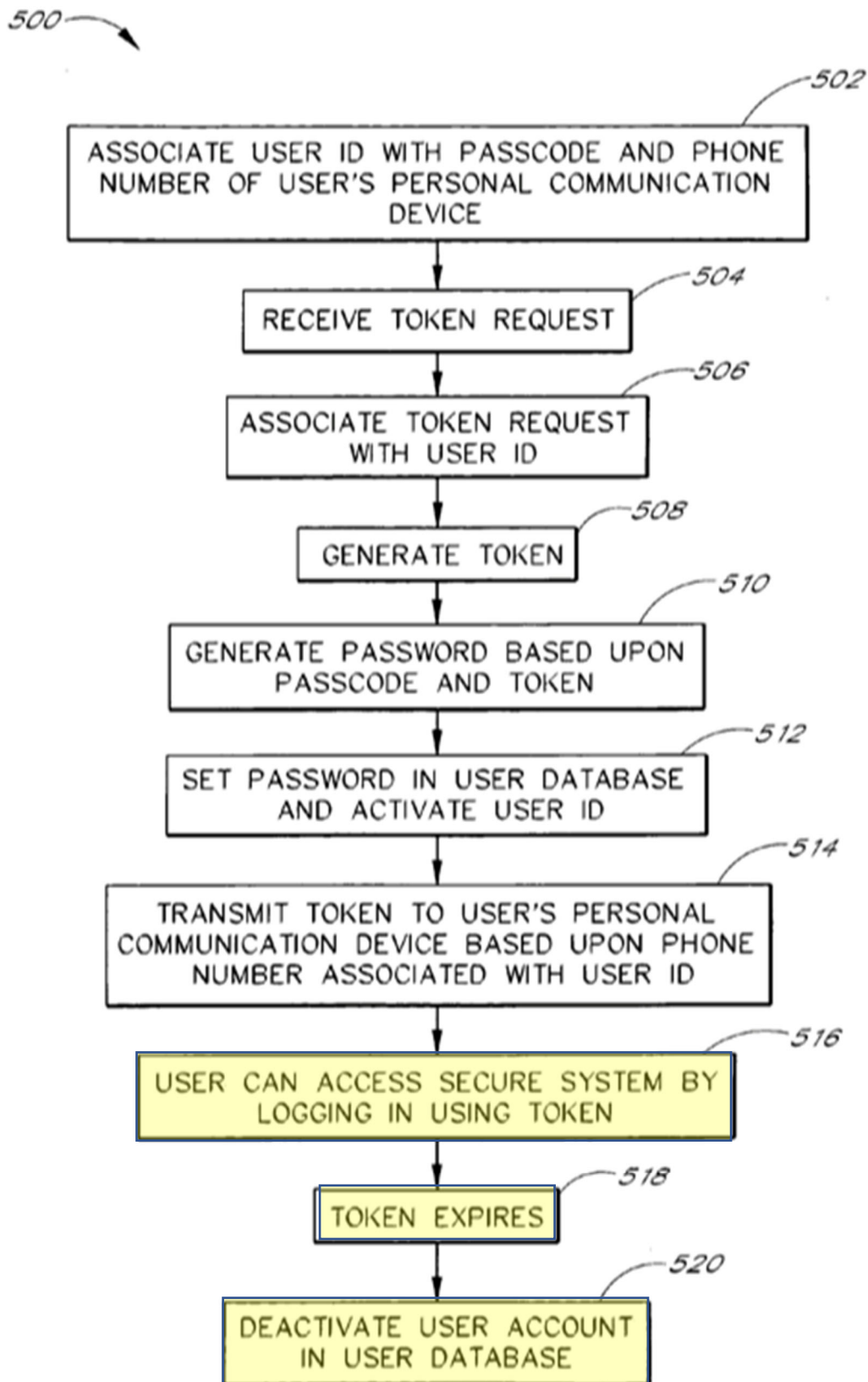


FIG. 5

Thus, *Veneklase*, in combination with *Jonsson*, teaches *wherein the user has an account on the secure computer network* (e.g., the user's password is found on the master password list), *wherein the authentication module* (e.g., code compare module 416) *activates access to the account in response to the password* (e.g., allows access if the response codes match) *and deactivates the account within a predetermined amount of time after activating the account* (e.g., denies entry if not received in the predetermined time window), *such that said account is not accessible through any password via the secure computer network* (e.g., not accessible even with the right password). EX1003, ¶¶106-111.

B. Ground 2: Claims 1, 3-6 Are Obvious over *Kew* in view of *Sormunen*

1. Overview of *Kew*

Kew discloses “a method of preventing unauthorised access to a host computer system (1) by a user at a remote terminal (2) is provided using paging system technology.” EX1007, Abstract, Fig. 1.

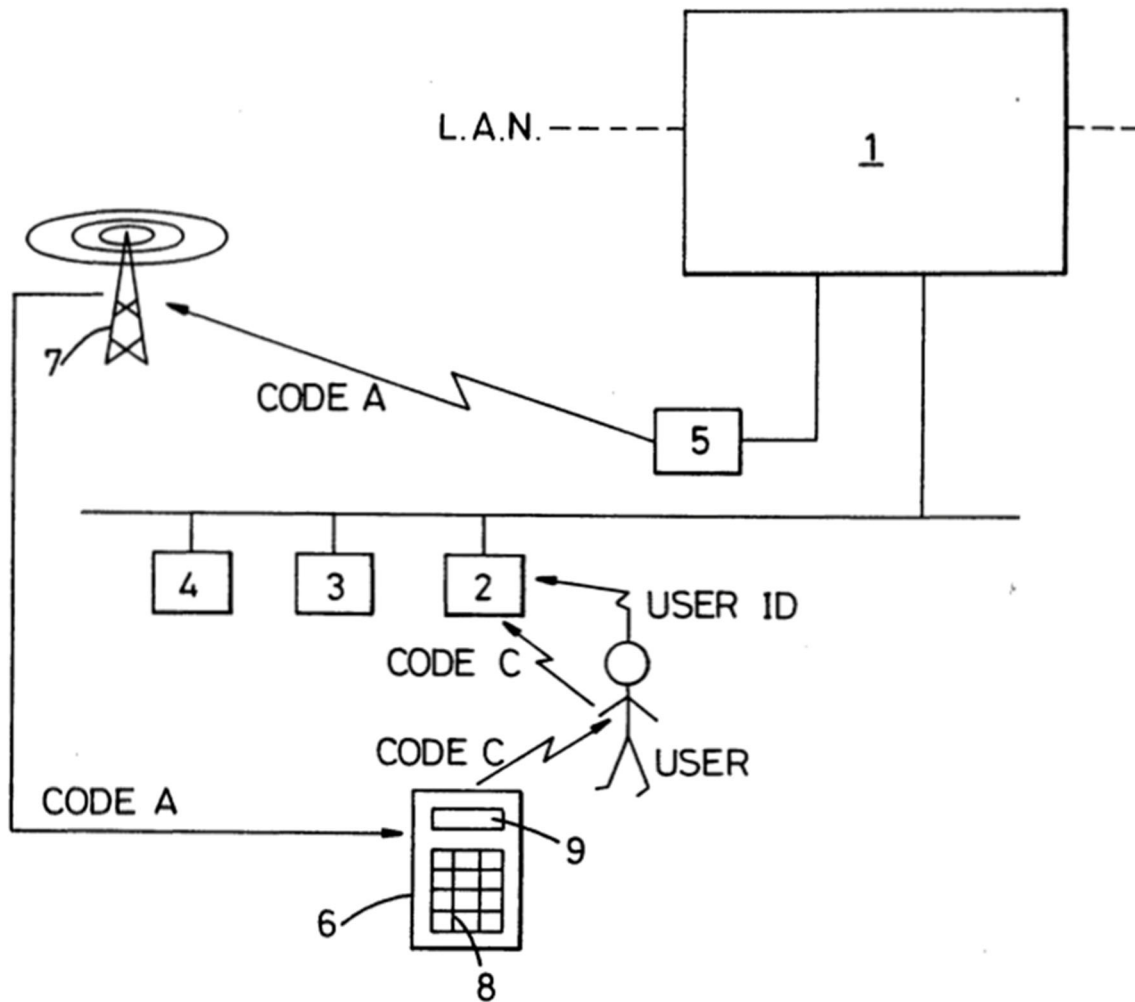
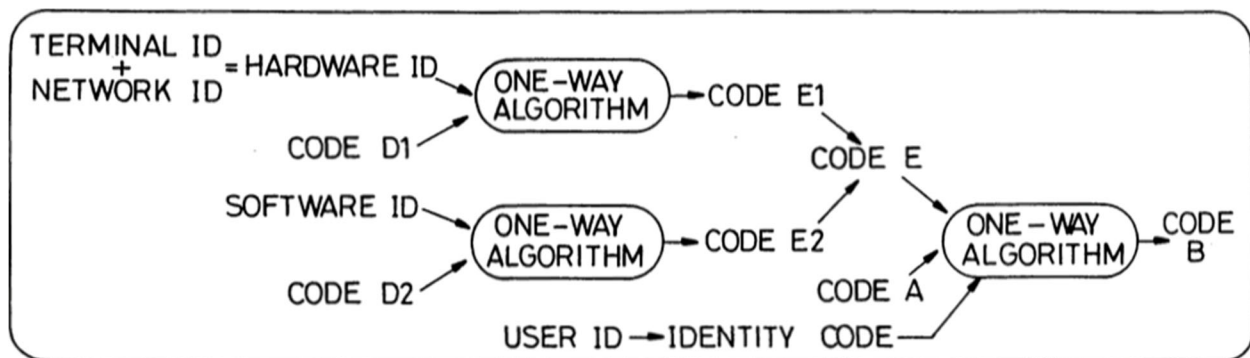


Fig. 1

For example, *Kew* discloses a system in which a user enters his user identification code, which can be his name or a PIN, into a terminal (e.g., 2, 3, 4), in order to gain access to a host computer system 1. EX1007, 7:34-8:2. Upon receiving this input, the security server 5, which “includes a database of all authorised users and their authorised receiver units 6,” “then generates a random code (Code A).”

EX1007, 8:2-6. Security server 5 then does two things with the random code, (1) it uses it and the identity code to produce a new transformed Code B, and (2) it “transmits the random code to a paging system 7 along with an identifier or identifying tag which can be recognized by the receiver unit 6.” EX1007, 8:5-23. Once the receiver unit 6 receives the random Code A, it “uses the received random number and the identity code stored in its own EPROM to produce a transformed code (Code C) via its own characteristic algorithm,” which is the same as the one used by the security server 5 to produce transformed code (Code B). EX1007, 8:33-36, Fig. 2.



“This transformed Code C is then displayed to the user...for a predetermined length of time.” EX1007, 8:36-9:3. Next, “terminal 2, at the behest of the security server 5 prompts the user to input the transformed Code C displayed by the receiver unit 6” and then “security server 5 compares the input Code C with the transformed code, Code B, it produced by encryption of the random code, Code A.” EX1007, 9:5-11. EX1003, ¶¶112-114.

2. Overview of *Sormunen*

Sormunen discloses “a method for obtaining at least one item of user specific data, wherein the user specific data is obtained at least partly by using paging or a short message service.” EX1008, Abstract. Specifically, *Sormunen* discloses that in order to obtain a password or list of passwords, “the user of the service sends a short message 2 from the paging terminal 3, such as a mobile station.” EX1008, 5:35-38, Fig. 2.

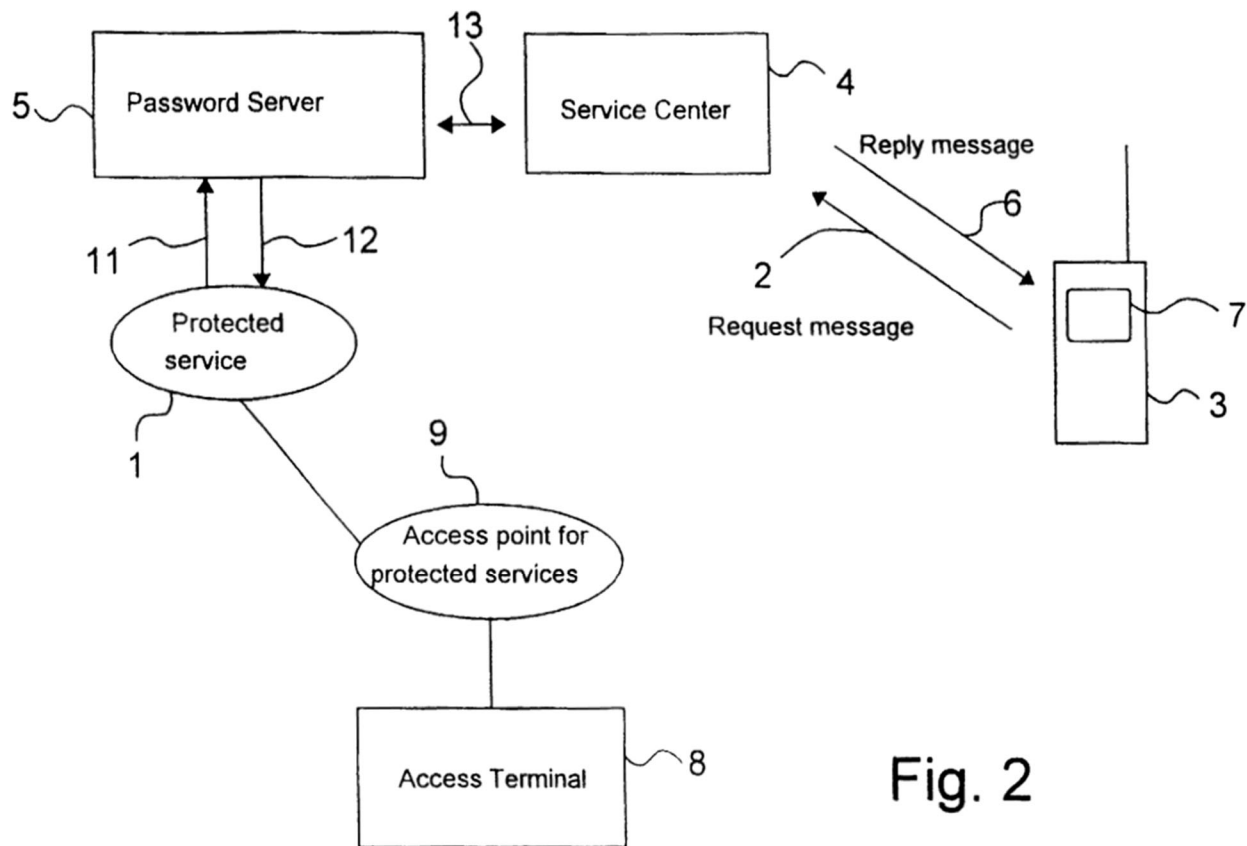


Fig. 2

Sormunen discloses that “the short message 2 includes a password request.” EX1008, 5:38-6:1. Next, the “paging service center 4 processes the incoming

message and forms according to it a data transmission connection to a password server 5 and transmits the inquiry to it,” which “processes the message and forms a reply message containing one or more passwords and the user name in case a new user is registered.” EX1008, 6:20-24. Eventually, “the reply message 6 arrived to the paging terminal 3 can be shown to the user for example by the display means 7 of a mobile station used as a paging terminal” and “[t]he user may subsequently start using the service 1.” EX1008, 8:4-7.

Sormunen notes that “[t]he present invention can be applied especially in such telecommunication systems in which it is possible to transmit short messages to a terminal belonging to the telecommunication system on the basis of a terminal key, such as a telephone number” and that “[t]his quality is included in mobile communication systems,” which “include for example a cellular system, a paging system, and a mobile phone system.” EX1008, 4:30-5:8. EX1003, ¶¶115-117.

3. Claim 5

[5.0] A user authentication system comprising

To the extent the preamble is deemed limiting, *Kew* teaches it; any alleged differences would have been obvious. EX1003, ¶¶120-121. *Kew* discloses “a method of **preventing unauthorized access to a host computer system.**” EX1007, Abstract; *see also* 1:3-15, Fig. 1.

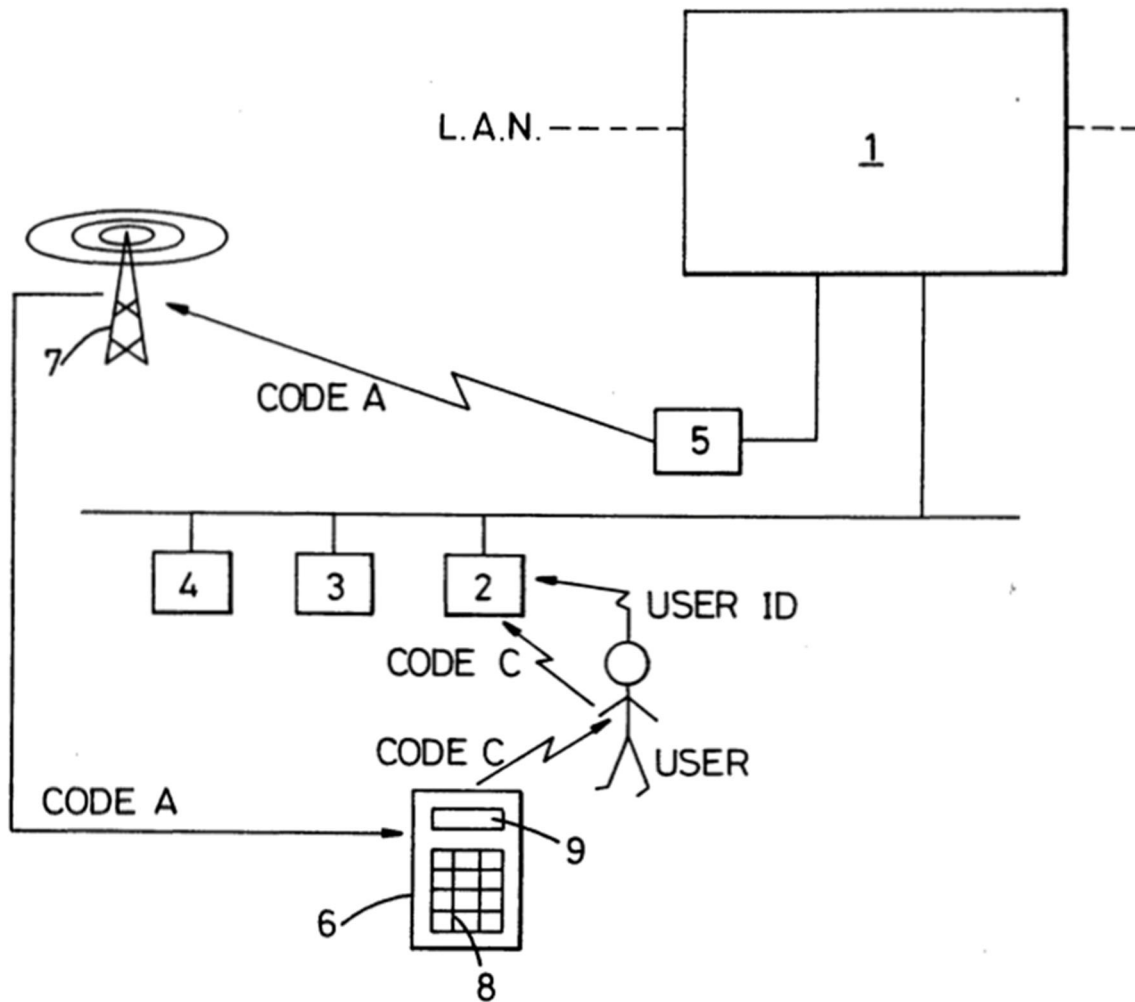


Fig. 1

Thus, *Kew* teaches *user authentication system* (e.g., authorization system).

EX1003, ¶¶120-121.

[5.1] a computer processor;

Kew teaches this limitation; any alleged differences would have been obvious.

EX1003, ¶¶122-124. Specifically, *Kew* discloses that terminal 2 operates “at the

behest of the **security server 5**,” and “also comprises a central processing unit (CPU) in its own right.” EX1007, 9:5-11, 10:4-12, Fig. 1.

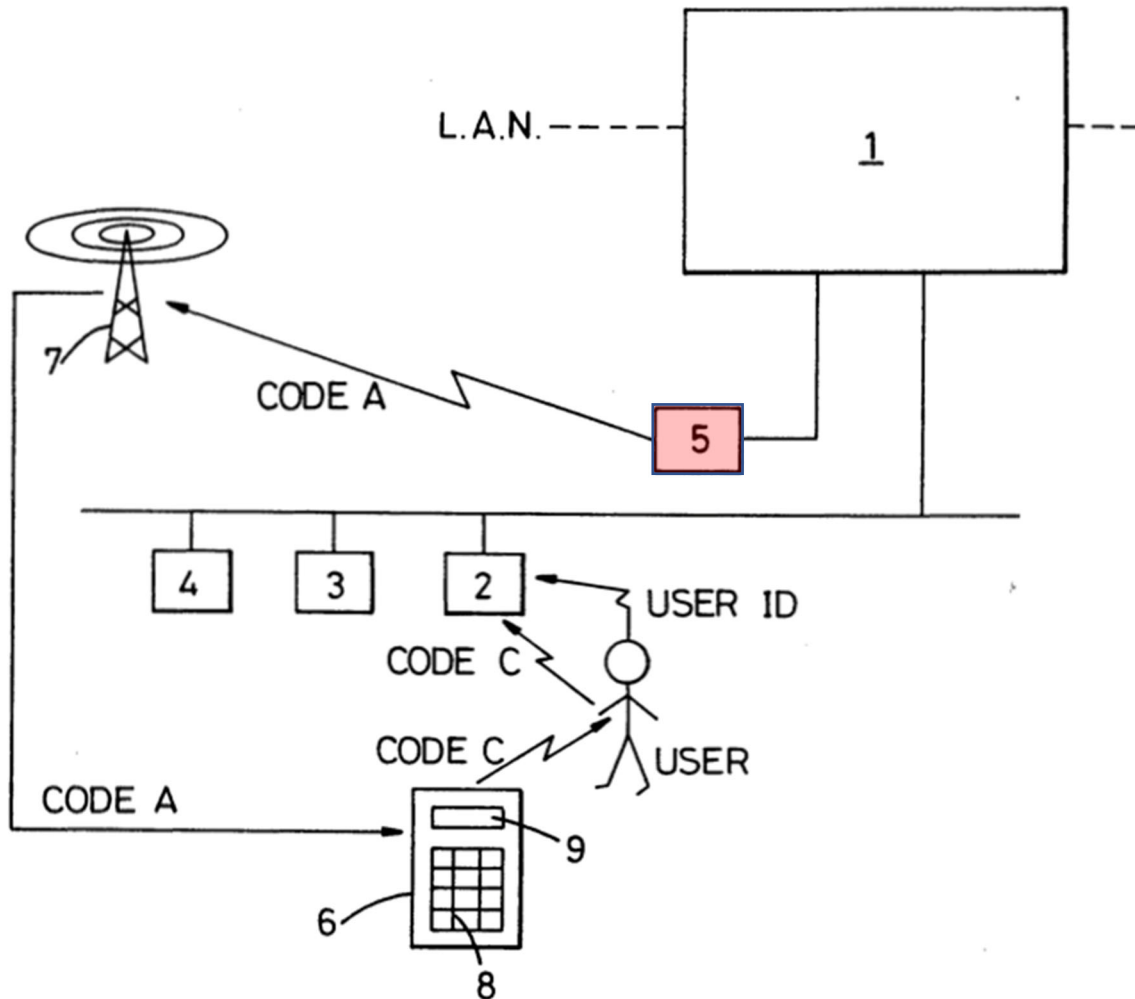


Fig. 1

Therefore, a POSITA would have understood *Kew*’s disclosure to teach that both the terminal 2 and the security server 5 contain a central processing unit.

EX1003, ¶¶122-123.

Thus, *Kew* teaches *a computer processor* (e.g., central processing unit).
EX1003, ¶¶122-124.

[5.2] a user database configured to associate a user with a personal communication device possessed by the user, said personal communication device configured to communicate over a cell phone network with the user authentication system;

Kew, alone or in combination with *Sormunen*, teaches this limitation; any alleged differences would have been obvious. EX1003, ¶¶125-130. *Kew* discloses that “security server 5 includes a **database of all authorised users and their authorised receiver units 6, and identifies the corresponding identity code for the appropriate receiver unit 6.**” EX1007, 8:2-5.

Kew additionally teaches a *personal communication device configured to communicate over a cell phone network with the user authentication system*. For example, *Kew* discloses that the **receiver unit 6** can be a **personal communication device**, such as a **pager**. See, e.g., EX1007, 8:12-23. *Kew* discloses that “**security server 5** also **transmits...to a paging system 7,**” and that transmitted information is then “**broadcast by the paging system 7, typically using a radiofrequency transmitter,** in a fashion similar to conventional paging systems.” EX1007, 8:13-19. “The receiver unit 6 will use the identifier to pick out the appropriate signal.” EX1007, 8:20-21. A POSITA would have understood that such communication channel is the same type of cell phone network disclosed in the ’658 patent, which repeatedly

makes clear that it covers both networks that communicate with cell phones and those that communicate with pagers. EX1001, 5:34-40 (“[t]he communication module 118 forwards tokens 156 to a text messaging service provider 104, which may be a pager or mobile phone service provider.”); *see also* Abstract, 1:10-11, 2:6-8, 2:28-31, 3:1-3, 4:13-17, 9:45-54; EX1003, ¶¶125-126. Thus, a POSITA would have understood that *Kew*’s disclosed communication network meets the requirements of a *cell phone network* as claimed in the ’658 Patent, i.e., a mobile device or pager service provider communication network. EX1003, ¶¶125-126.

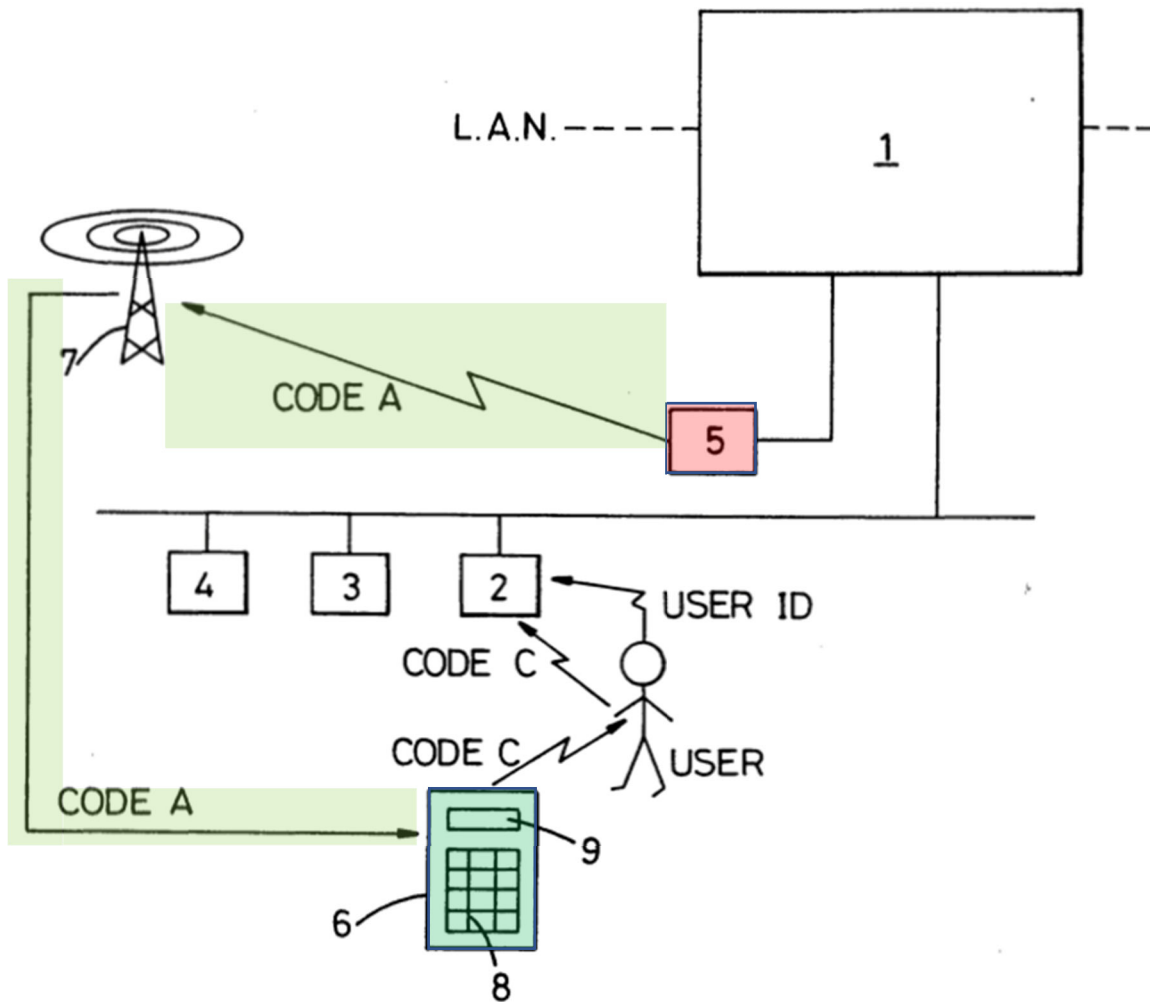


Fig. 1

To the extent it is argued that the pager network disclosed in *Kew* does not satisfy the cell phone network limitation, a POSITA would have found it obvious to implement the authentication system of *Kew* using a cell phone network. EX1003, ¶¶127-128; *KSR*, 550 U.S. at 418-19. Indeed, *Kew* explicitly contemplates that the device 6 and the security server 5 communicate via “radiofrequency transmitter(s).”

EX1007, 8:12-23. While the example provided in *Kew* is a pager system, a POSITA would have found it obvious to use a cell phone network, which is another type of communication that utilizes radiofrequency transmission. EX1003, ¶¶127-128. In addition, it would have been obvious to use a cell phone network to send *Kew*'s random code (Code A) because doing so would have made the system available to even more users in more locations, which is one of the intentions of the reference. *Id.* It would also have been obvious because it would have enabled users to use their cell phones to authenticate their access, which many users would prefer because they provide for larger screens and are thus easier to view. *Id.* A POSITA would have had a reasonable expectation of success in modifying *Kew*'s authentication system to use a cellular network instead of a pager network because they operate similarly, many times using the same protocols, and would just involve swapping out devices and making some software configuration changes. *Id.*

Thus, *Kew* teaches *a user database configured to associate a user with a personal communication device possessed by the user (e.g., a database of all authorized users and their authorized receiver units), said personal communication device (e.g., receiver unit 6) configured to communicate over a cell phone network (e.g., communicates over a radiofrequency transmission network) with the user authentication system (e.g., security server 5).* EX1003, ¶¶125-128.

To the extent it is argued *Kew* does not teach or render obvious the use of a cell phone network, *Sormunen* discloses a *personal communication device* (e.g., paging device 3) *configured to communicate over a cell phone network* (e.g., cellular network). EX1003, ¶¶129-130. Specifically, *Sormunen* discloses that in order to obtain a password or list of passwords, “the user of the service sends a short message 2 from the **paging terminal 3, such as a mobile station.**” EX1008, 5:35-38, Fig. 2.

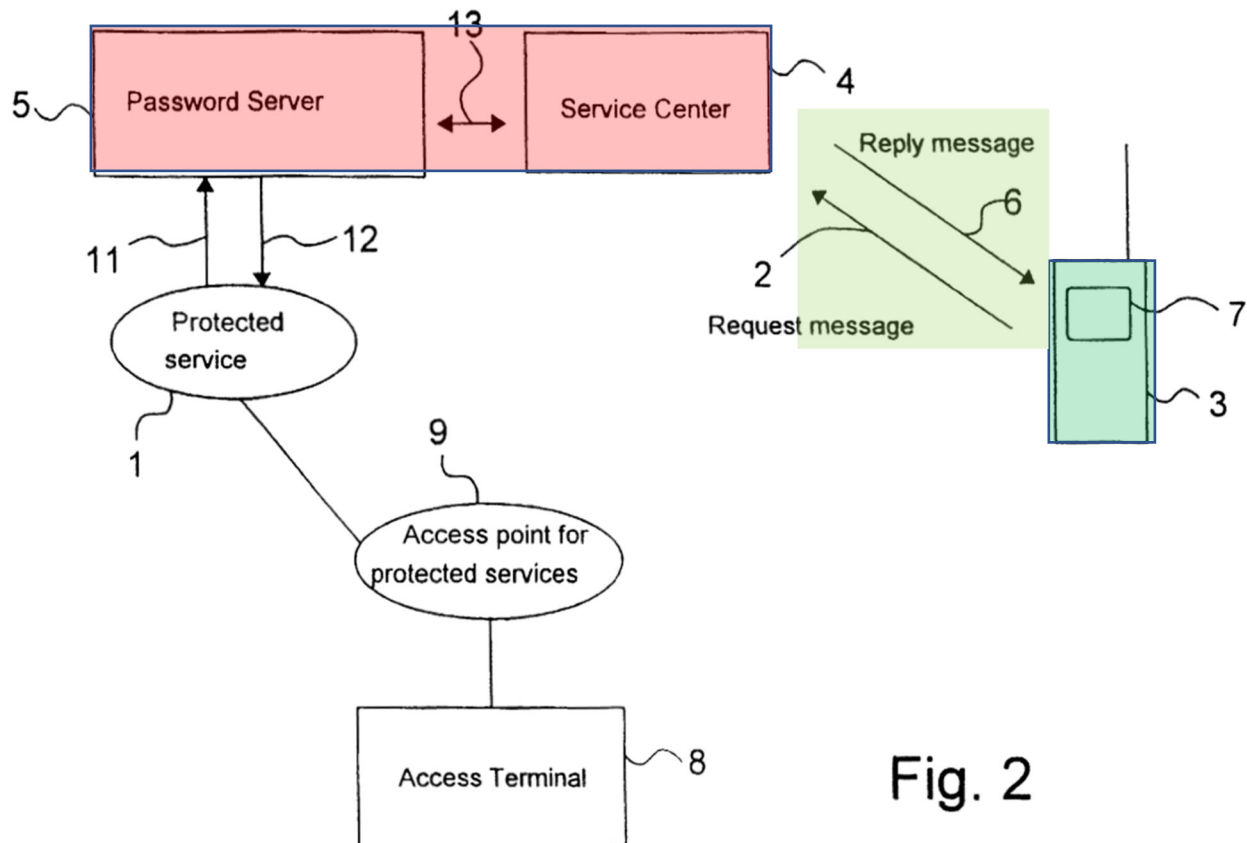


Fig. 2

Sormunen discloses that “[t]he present invention can be applied especially in such telecommunication systems in which it is possible to transmit short messages to a terminal belonging to the telecommunication system on the basis of a terminal

key, such as a telephone number” and that “[t]his quality is included in mobile communication systems,” which “include for example a **cellular system, a paging system, and a mobile phone system.**” EX1008, 4:30-5:8. *Sormunen* discloses that a “cellular system, such as the GSM system, is a mobile communication system in which a **cellular network** is used.” *Id.*

Motivations to Combine *Kew* and *Sormunen*

It would have been obvious to incorporate *Sormunen*’s teachings related to an authentication system in which a paging device communicates with the authentication system via a cellular network into *Kew*’s authentication system that utilizes conventional paging systems to communicate between a receiver unit and a security server. EX1003, ¶¶131-135. *Kew* teaches a system in which a random code can be sent from a security server to a receiver unit via “conventional paging systems.” *See, e.g.*, EX1007, 8:12-23. *Sormunen* discloses a similar authentication system that allows a paging device to communicate with the authentication system via a cellular network, such as the well-known GSM system. *See, e.g.*, EX1008, 4:30-5:8. A POSITA would have been motivated to make such a combination because it would have allowed *Kew*’s authentication system to operate on the well-known and ubiquitous GSM system. EX1003, ¶131. Furthermore, a POSITA would have been motivated to make such a combination because implementing *Kew*’s authentication system on a cellular network, as disclosed in *Sormunen* would allow

for two way communication between the receiver unit and the security server, and thus allow the user to request a random code via the receiver unit, as well as the terminal, which is precisely what is disclosed in *Sormunen*. See, e.g., EX1007, 7:34-35; EX1003, ¶131.

Furthermore, *Kew* explicitly provides a teaching, suggestion, and motivation for combining it with an authentication system that operates on other types of networks, such as those taught in *Sormunen*, because it explicitly discloses the use of a radiofrequency transmitter, which is also used in other systems, such as the GSM network. See, e.g., EX1007, 8:15-19; *KSR Intern. Co. v. Teleflex Inc.*, 550 U.S. 398, 418-19 (2007). Thus, a POSITA would have been motivated to use *Kew*'s authentication system in conjunction with receiver units that can operate on a cellular network, such as described in *Sormunen*, to provide additional flexibility and features. EX1003, ¶132.

A POSITA would further be motivated to combine *Kew* and *Sormunen* because the combination merely uses a known technique to improve similar devices in the same way. See *KSR*, 550 U.S. at 401. For instance, a POSITA would have been motivated to utilize the cellular network functionality of *Sormunen* in the system of *Kew* because it would have been used in the same way, i.e., to allow communication between a mobile device unit and a central server. EX1003, ¶133. As discussed above, *Kew* discloses the use of radiofrequency transmitters operating

via conventional systems (e.g., paging systems), so it would have been obvious for a POSITA to combine it with *Sormunen*, which teaches that such a system can operate on paging systems as well as cellular systems and mobile systems. *See, e.g.*, EX1008, 40:30-5:9; EX1003, ¶133.

A POSITA would have had a reasonable expectation of success in modifying *Kew*'s authentication system, which uses a conventional paging network, to use a conventional cellular network, such as GSM, as taught by *Sormunen*. EX1003, ¶¶131-134.

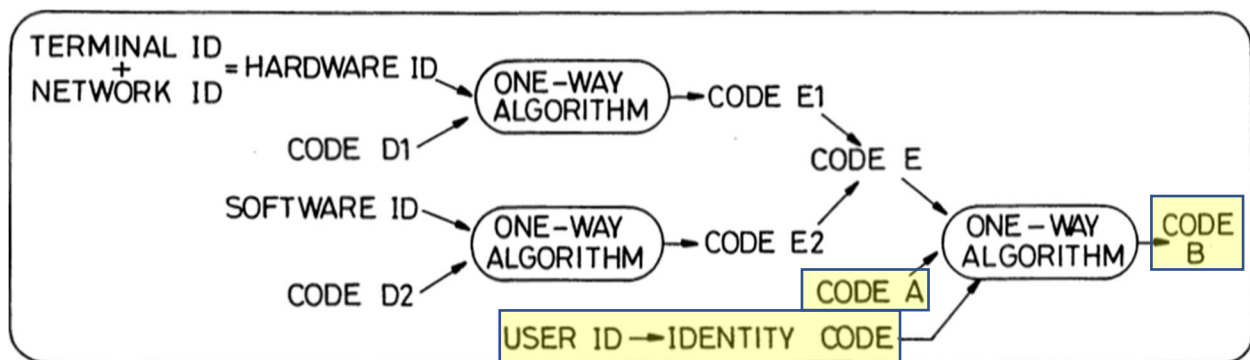
Therefore, a POSITA would have been motivated to modify, and would have had a reasonable expectation of success in modifying, *Kew*'s authentication system to include *Sormunen*'s teachings related to the use of a cellular network. EX1003, ¶¶131-135. Thus, *Kew*, in combination with *Sormunen*, teaches this limitation.

[5.3] a control module executed on the computer processor configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a password associated with the user to be the new password;

Kew teaches this limitation; any alleged differences would have been obvious. EX1003, ¶¶136-140. *Kew* discloses that the security server creates a new password (e.g., transformed code (Code B)) based on a token (e.g., random code (Code A)) and a passcode (e.g., identity code) via an encryption mechanism. Specifically, *Kew*

discloses that after the user enters his user identification code, “the security server 5 then **generates a random code (Code A)** and subjects this number to an encryption using the same one-way algorithm as is stored in the user’s receiver 6 together with the corresponding **identity code**” to create a “**transformed code (Code B).**” EX1007, 8:5-10. *Kew* further discloses that “the security server 5 also transmits the random code to a paging system 7 along with an identifier or identifying tag which can be recognized by the receiver unit 6.” EX1007, 8:12-15.

Kew discloses that after the receiver unit 6 receives the random number, it “uses the received random number and the identity code stored in its own EPROM to produce a transformed code (Code C) via its own characteristic algorithm,” which is the same as the one used by the security server 5 to produce transformed code (Code B). EX1007, 8:33-36. Although Figure 2 includes a more complicated embodiment utilizing additional Code E, the simpler embodiment being discussed here shows how new password Code B is created based on both the User ID/Identity Code and randomly generated Code A. EX1007, Fig. 2.



As discussed above, Code A is a “random number” generated by security server 5, and thus not known to the user prior to it being sent to the receiver unit. The identity code, on the other hand, “should preferably be treated by the user as a secret code” and “is thus comparable with a personal identification number (PIN) familiar from many other contexts,” and is thus known to the user beforehand. EX1007, 3:8-12. The identity “code may take any suitable form, for example his actual name or preferably a more secure code such as a PIN.” EX1007, 7:36-8:2. A POSITA would have understood that PINs that are “treated by the user as a secret code” are known to the user in order for them to be treated as such. EX1003, ¶¶136-138.

Kew additionally discloses that “terminal 2, at the behest of the security server 5 prompts the user to input the transformed Code C displayed by the receiver unit 6” and then “security server 5 **compares the input Code C with the transformed code, Code B**, it produced by encryption of the random code, Code A.” EX1007, 9:5-11. Therefore, a POSITA would have understood that *Kew*’s security server is setting transformed Code B that it created by encryption *to be the new password*, i.e., the password against which the user’s input code (Code C) is to be measured against. EX1003, ¶¶136-139.

Thus, *Kew* teaches *a control module executed on the computer processor (e.g., a portion of security server 5) configured to create a new password (e.g.,*

transformed code (Code B)) *based at least upon a token* (e.g., random code (Code A)) *and a passcode* (e.g., identity code), *wherein the token is not known to the user* (e.g., random code generated by server) *and wherein the passcode is known to the user* (e.g., his actual name or PIN), *the control module further configured to set a password associated with the user to be the new password* (e.g., using transformed code (Code B) as the new password). EX1003, ¶¶136-140.

[5.4] a communication module configured to transmit the token to the personal communication device through the cell phone network, and

Kew teaches this limitation; any alleged differences would have been obvious. EX1003, ¶¶141-143. Specifically, *Kew* discloses that its system includes “transmitting Code A [the randomly generated token] via a paging system, to a receiver held by the user.” EX1007, 1:31-32. As discussed with respect to element [5.2], “the security server 5 also transmits the random code to a paging system 7” and “the identifying tag and the random code are then broadcast by the paging system 7, typically using a radiofrequency transmitter, in a fashion similar to conventional paging systems.” *Id.*, 8:12-19.

As discussed above, the claimed *cell phone network* must at least include mobile device and pager service provider communication networks. *See, e.g.*, EX1001, 5:32-40, 9:45-54, 4:13-17, 3:1-3, 2:28-31, 2:6-8, 1:7-11. Indeed, the ’658 Patent discloses an embodiment in which “the communication module 118 is a

phone dialer 622, the personal communication device 106 is a pager 624, and the text messaging service provider is a paging service 626.” EX1001, 10:31-34. This is very similar to what is disclosed in *Kew*. Thus, it is clear that the “cell phone network” claimed in the ’658 Patent also includes the pager network, as disclosed in *Kew*. EX1003, ¶¶141-142, 25.

Thus, *Kew* teaches *a communication module* (e.g., a portion of security server 5) *configured to transmit the token to the personal communication device through the cell phone network* (e.g., transmit the random code (Code A) to a receiver via a paging system). EX1003, ¶¶141-143.

[5.5] an authentication module configured to receive the password from the user through a secure computer network, said secure computer network being different from the cell phone network,

Kew teaches this limitation; any alleged differences would have been obvious. EX1003, ¶¶144-146. *Kew* discloses *an authentication module* (e.g., a portion of security server 5) *configured to receive the password from the user through a secure computer network* (e.g., by prompting the user to input Code C). Specifically, *Kew* discloses that “the receiver unit 6 therefore uses the received random number and the identity code stored in its own EPROM to produce a transformed code (Code C),” which is “then displayed to the user.” EX1007, 8:33-9:3. *Kew* further discloses that “the terminal 2, at the behest of the security server 5 **prompts the user to input**

the transformed Code C displayed by the receiver unit 6.” EX1007, 9:5-7. *Kew* discloses that this information is entered into a remote terminal, which is connected to the host computer system “via a telephone line link.” EX1007, 7:10-14, Fig. 1.

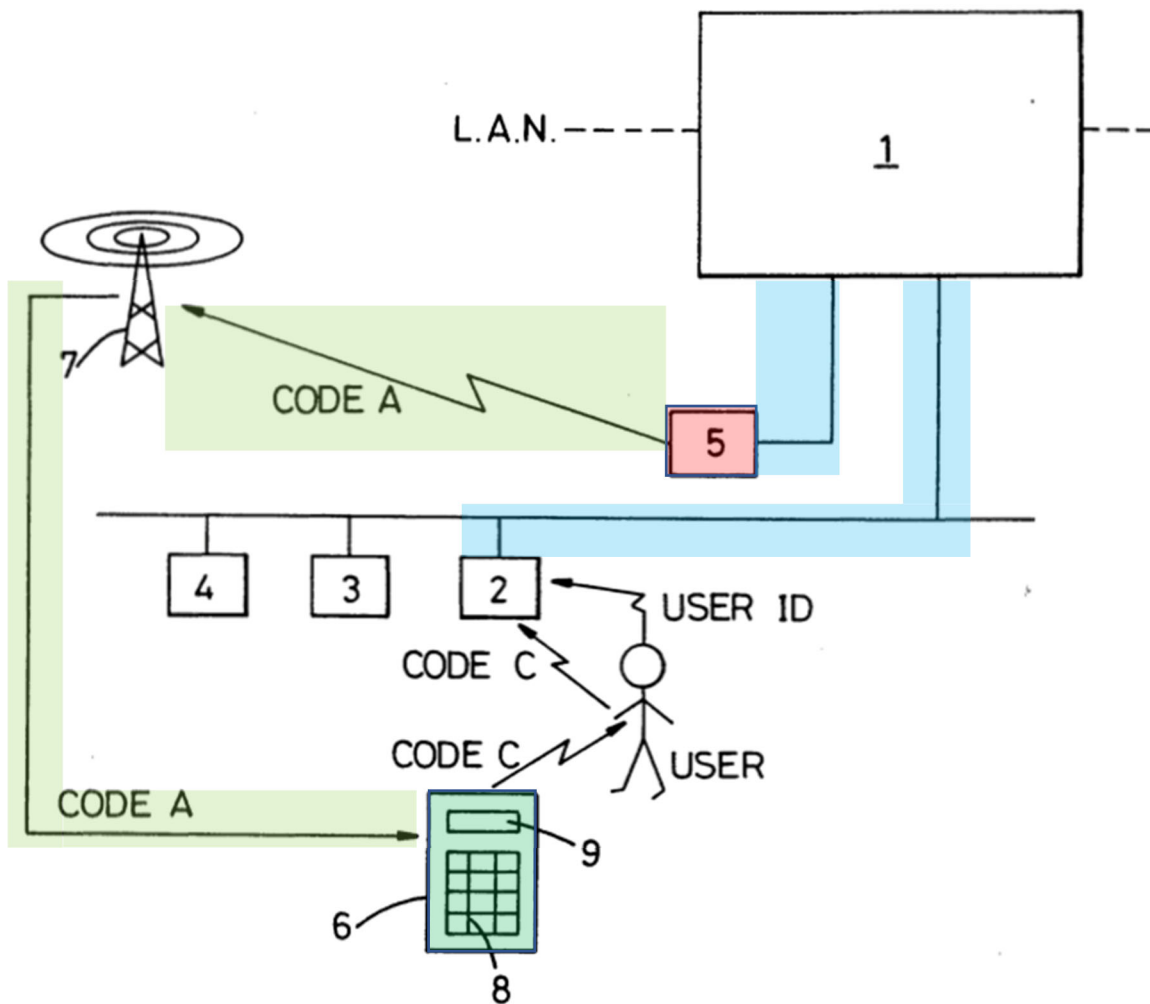


Fig. 1

A POSITA would have understood that this connection, which is different from the pager network connecting the system to the personal receiver device, is

secure because the connection requires that a user verify his identity. EX1003, ¶¶144-145. Specifically, *Kew* discloses “a computer security system...for preventing unauthorized access to a host computer system,” which makes it a *secure computer system*. EX1007, 1:3-5. *Kew* further discloses that “[t]o gain access to the host system 1, a user at one of the terminals, say terminal 2, must first verify his or her identity by satisfying a security barrier system or security server 5, which is effectively interposed between the remote terminals 2, 3, 4 and the host system 1.” EX1007, 7:10-18. This is similar to what the ’465 Patent describes, which is “for a secure system, such as a computer system.” EX1001, 1:63-65; *see also* 2:49-3:3; 4:9-26.

Thus, *Kew* teaches *an authentication module* (e.g., a portion of security server 5) *configured to receive the password from the user through a secure computer network* (e.g., by prompting the user to input Code C), *said secure computer network being different from the cell phone network* (e.g., a telephone line link). EX1003, ¶¶144-146.

[5.6] wherein the user has an account on the secure computer network, wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account, such that said account is not

accessible through any password via the secure computer network.

Kew teaches this limitation; any alleged differences would have been obvious. EX1003, ¶¶147-152. *Kew* discloses *wherein the authentication module (e.g., a portion of security server 5) activates access to the account in response to the password (e.g., if Code B and Code C are identical, access to the host system 1 is permitted).* Specifically, *Kew* discloses that once the user has input the transformed Code C, **“the security server 5 compares the input Code C with the transformed code, Code B”** and **“[i]f Code B and Code C are identical, access to the host system 1 is permitted.”** EX1007, 9:5-11; *see also* 1:36-2:3.

In addition, *Kew* discloses *wherein the user has an account on the secure computer network (e.g., the user is listed as an authorized user in security server 5’s database).* Specifically, *Kew* discloses that this system is implemented only when the user is listed as an authorized user in security server 5’s database. EX1007, 8:2-5 (“The security server 5 includes a database of all authorised users and their authorised receiver units 6, and identifies the corresponding identity code for the appropriate receiver unit 6.”). Thus, a POSITA would have understood that in order for the user to be listed in the database as an authorized user, that user needs to have an account on the secure computer network. EX1003, ¶¶147-148.

Additionally, *Kew* discloses that its system *deactivates the account within a predetermined amount of time after activating the account* (e.g., enabled for a predetermined period), *such that said account is not accessible through any password via the secure computer network* (e.g., an unauthorised user cannot gain access to the system even if he has possession of the receiver and knows the user identification code). Specifically, *Kew* discloses that **“the receiver can only be enabled for a predetermined period to permit it to transform the received Code A to the transformed Code C by input of a second user identification code by the user.”** EX1007, 3:14-17. *Kew* explains that after that predetermined period of time, “an unauthorised user cannot gain access to the system even if he has possession of the receiver and knows the user identification code without knowledge of the second identification or activation code.” EX1007, 3:19-23.

Kew further discloses that after the receiver device uses the received random number and the identity code to produce the transformed Code C, “[t]his **transformed Code C is then displayed to the user on a display means 9...for a predetermined length of time such as five minutes.**” EX1007, 8:33-9:3. A POSITA would have understood that by only displaying the transformed Code C that the user needs to input into the terminal to gain access to the system for a predetermined period of time, that has the effect of deactivating the account by not allowing access to the account via any password. EX1003, ¶¶149-151. Once the

predetermined period of time has run, the display is no longer visible and the user would have to reactivate the account by starting the process over and having the system send a new randomly generated Code A. *Id.*

Kew's teaching is within the scope of the recited deactivating limitation because it is nearly identical to how this limitation is described in the '658 Patent. Indeed, the '658 Patent discloses in Figure 5 that the “user can access secure system by logging in using token” in step 516, but if the “token expires” in step 518, it “deactivate[s] user account in user database.” EX1001, Fig. 5; 9:61-64 (“At a step 518, if the token has an expiry time, the token 156 expires. At a step 520, upon expiration of the token 156, the control module 402 deactivates the user account in the user database 114.”).

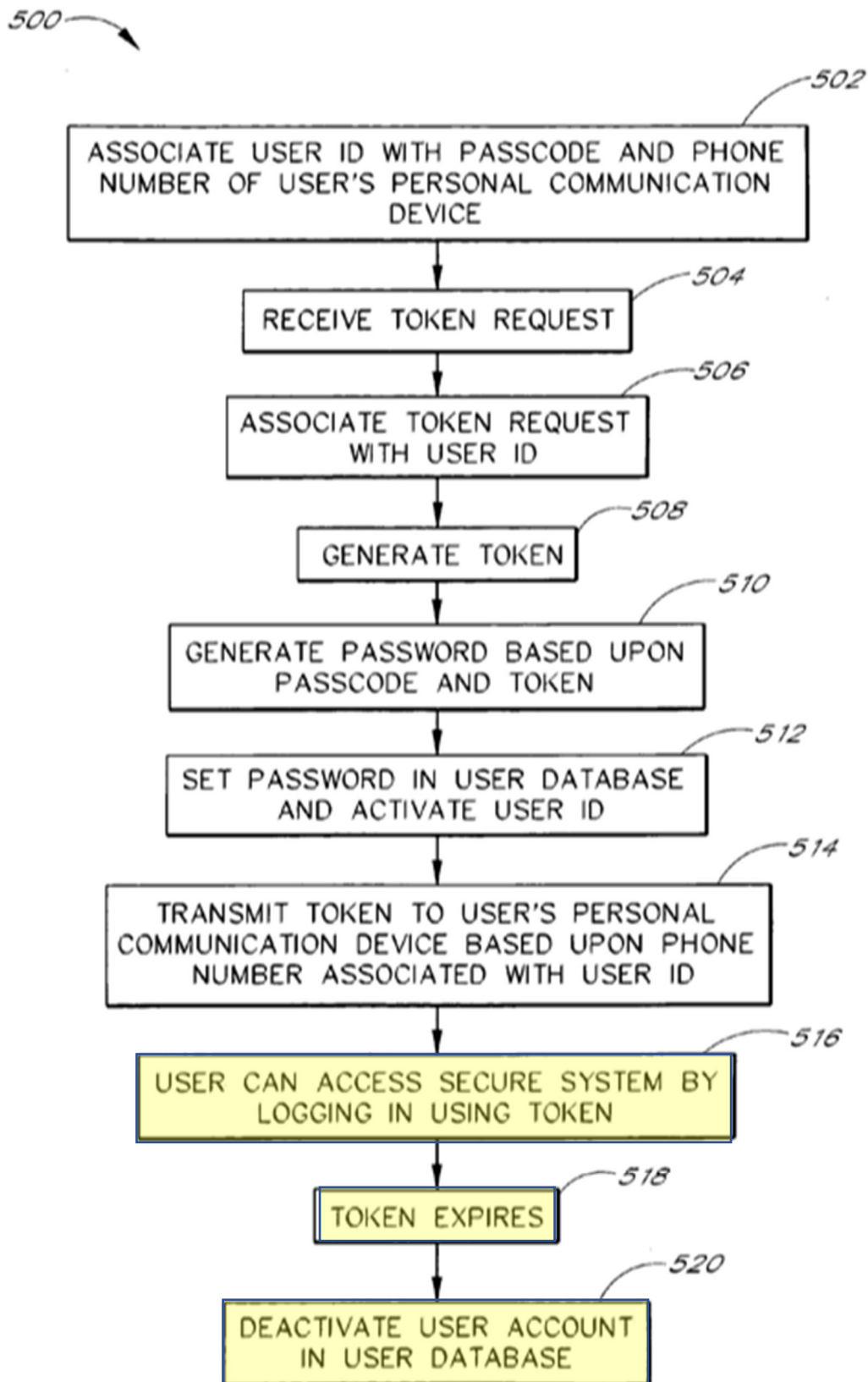


FIG. 5

Thus, *Kew* teaches *wherein the user has an account on the secure computer network* (e.g., the user is listed as an authorised user in security server 5's database), *wherein the authentication module* (e.g., a portion of security server 5) *activates access to the account in response to the password* (e.g., if Code B and Code C are identical, access to the host system 1 is permitted) *and deactivates the account within a predetermined amount of time after activating the account* (e.g., enabled for a predetermined period), *such that said account is not accessible through any password via the secure computer network* (e.g., an unauthorised user cannot gain access to the system even if he has possession of the receiver and knows the user identification code). EX1003, ¶¶147-152.

4. Claim 6

[6.0] The system of claim 5,

Kew in view of *Sormunen* renders obvious claim 5. Sec. III.B.3.

[6.1] 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.

Kew teaches this limitation; any alleged differences would have been obvious. EX1003, ¶¶153-155. *Kew* discloses that “[w]hen the user seeks access to the host system 1 via the terminal 2, he enters his user identification code.” EX1007, 7:34-35. Upon receiving the user identification code, “security server 5 then generates a random code (Code A) and subjects this number to an encryption using the same

one-way algorithm as is stored in the user's receiver 6 together with the corresponding identity code,” and in doing so, “transformed code (Code B) is produced.” *Id.*, 8:5-10. Therefore, a POSITA would have understood that the user's submission of his user identification code serves as a request for the token (i.e., random Code A) to be sent to their personal receiver device and the security server also creates the new password (i.e., transformed Code B) in response to the request. EX1003, ¶¶153-155.

Thus, *Kew* teaches *wherein the communication module is further configured to receive a request from the user for the token* (e.g., receives a communication that leads to the creation of random Code A), *and wherein the control module is further configured to create the new password in response to the request* (e.g., transformed Code B is produced in response). *Id.*

5. Claim 1

Most limitations of claim 1 are substantively similar to claim 5. Therefore, these limitations are obvious for the same reasons as the corresponding limitations in claim 5, charted below. The limitations with differences are also obvious for the reasons discussed below. Thus, claim 3 is obvious over *Kew* in view of *Sormunen*. EX1003, ¶¶156-160.

Claim 1		Cross-References
[1.0]	<i>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:</i>	[5.0], [5.5], [5.6]
[1.1]	<i>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;</i>	[5.2], [5.5]
[1.3]	<i>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;</i>	[5.3]
[1.4]	<i>setting a password associated with the user to be the new password;</i>	[5.3]
[1.5]	<i>activating access the user account on the first secure computer network;</i>	[5.6]
[1.6]	<i>transmitting the token to the personal communication device;</i>	[5.4]
[1.7]	<i>receiving the password from the user via the first secure computer network; and</i>	[5.5]
[1.8]	<i>deactivating access to the user account on the first secure computer network within a predetermined amount of time after said activating, such that said user account is not accessible through any password, via said first secure computer network.</i>	[5.6]

[1.2] receiving a request from the user for a token via the personal communication device, over the second network;

Kew, in combination with *Sormunen*, teaches this limitation; any alleged differences would have been obvious. EX1003, ¶¶157-160. Specifically, *Sormunen* discloses that in order to obtain a password or list of passwords, “the user of the service **sends a short message 2 from the paging terminal 3, such as a mobile station.**” EX1008, 5:35-38, Fig. 2.

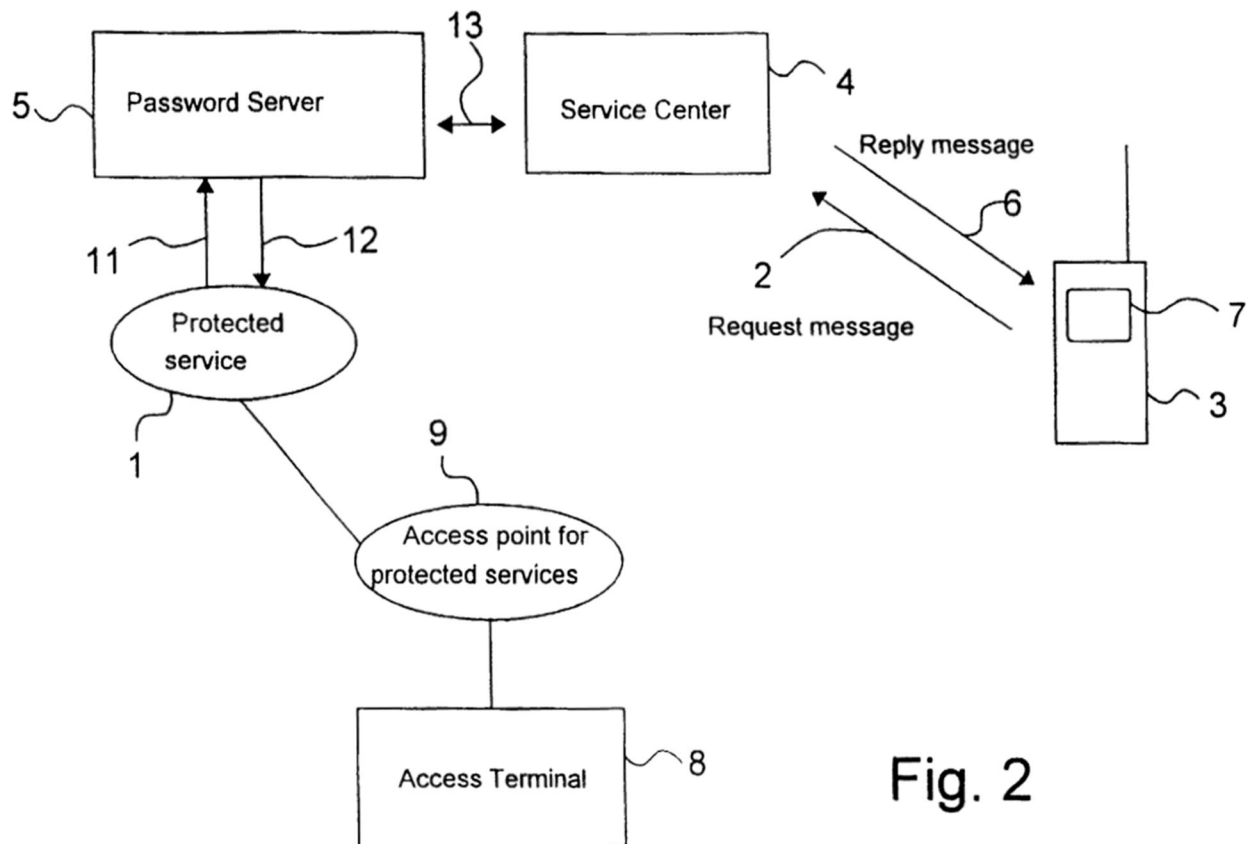


Fig. 2

Sormunen discloses that “the short message 2 includes a **password request.**” EX1008, 5:38-6:1. In the combination with *Kew* described with respect to claim 5, A POSITA would have understood that this request would be for a token (e.g., random code (Code A)). EX1003, ¶¶157-158, 129-135.

Next, the “paging service center 4 processes the incoming message and forms according to it a data transmission connection to a password server 5 and transmits the inquiry to it,” which “processes the message and forms a reply message containing one or more passwords and the user name in case a new user is registered.” EX1008, 6:20-24. *Sormunen* notes that “[t]he present invention can be applied especially in such telecommunication systems in which it is possible to transmit short messages...on the basis of a terminal key, such as a telephone number” and that “[t]his quality is included in mobile communication systems,” which “include for example a **cellular system, a paging system, and a mobile phone system.**” EX1008, 4:30-5:8.

Thus, *Kew*, in combination with *Sormunen*, teaches *receiving a request from the user for a token* (e.g., a password request) *via the personal communication device* (e.g., receiver unit/paging terminal), *over the second network* (e.g., cellular network). EX1003, ¶¶157-160.

6. Claim 3

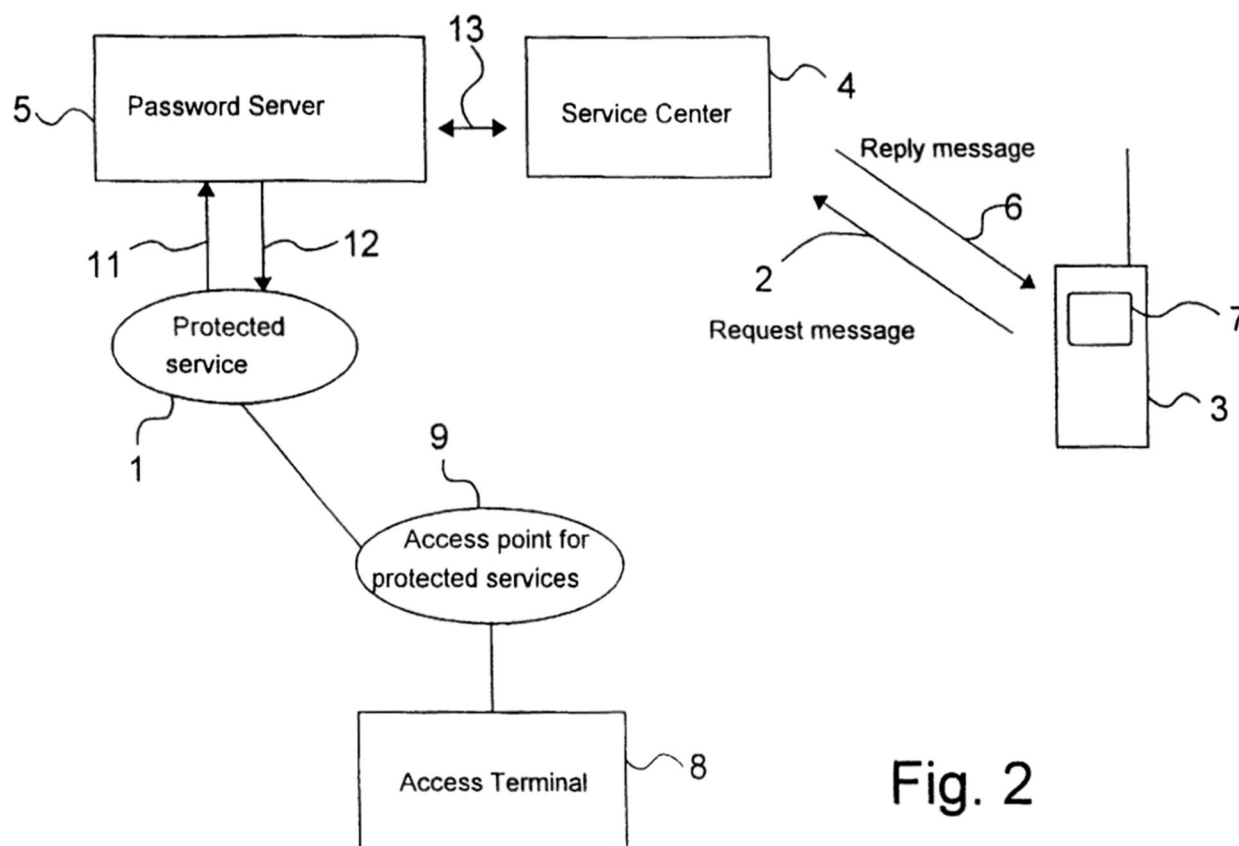
[3.0] The method of claim 1,

Kew in view of *Sormunen* renders obvious claim 1. Sec. III.B.5.

[3.1] wherein the personal communication device is a mobile phone.

Kew, in combination with *Sormunen*, teaches this limitation; any alleged differences would have been obvious. EX1003, ¶¶161-164. *Sormunen* discloses

that *the personal communication device* is a “paging terminal 3, such as a mobile station.” EX1008, 5:35-38, Fig. 2.



Sormunen discloses that “[t]he present invention can be applied especially in such telecommunication systems in which it is possible to transmit short messages...on the basis of a terminal key, such as a telephone number” and that “[t]his quality is included in mobile communication systems,” which “include for example a cellular system, a paging system, and a **mobile phone system**.” EX1008, 4:30-5:8. Thus, a POSITA would understand *Sormunen* to disclose that the mobile station can be a mobile phone. EX1003, ¶¶162-163.

Thus, *Kew*, in combination with *Sormunen*, teaches *wherein the personal communication device is a mobile phone* (e.g., mobile station that operates on mobile phone system). EX1003, ¶¶161-164.

7. Claim 4

[4.0] The method of claim 1,

Kew in view of *Sormunen* renders obvious claim 1. Sec. III.B.5.

[4.1] wherein the personal communication device is a pager.

Kew, alone or in combination with *Sormunen*, teaches this limitation; any alleged differences would have been obvious. EX1003, ¶¶165-167. As discussed with respect to claim 5, *Kew* discloses that *the personal communication device is a pager*. See, e.g., EX1007, 8:12-23. *Kew* discloses that “security server 5 also transmits...to a paging system 7,” and that transmitted information is then “broadcast by the paging system 7, typically using a radiofrequency transmitter, in a fashion similar to conventional paging systems.” EX1007, 8:13-19. “The receiver unit 6 will use the identifier to pick out the appropriate signal.” EX1007, 8:20-21. *Sormunen* also discloses that *the personal communication device is a pager* (e.g., a “paging terminal 3, such as a mobile station.”) EX1008, 5:35-38, Fig. 2.

Thus, *Kew*, alone or in combination with *Sormunen*, teaches *wherein the personal communication device is a pager* (e.g., receiver that receives pages). EX1003, ¶¶165-167.

C. Analogous Art

Veneklase, Jonsson, Kew, and Sormunen are analogous art. All are in the same field of endeavor as the '658 Patent because all three relate to authentication systems utilizing personal communication devices, such as pagers. *See, e.g.*, EX1001, 1:7-11 (“relates generally to the authentication of user of secure systems and, more particularly,...to a system through which user tokens required for user authentication are supplied through personal communication devices such as mobile telephones and pagers”); EX1005, Abstract (“computer security systems are described and which are adapted to grant an authorized individual access to a secured domain” by use of a pager); EX1006, Abstract (“[a]uthorization for a user to use a service is provided by a modified pager.”); EX1007, Abstract (“method of preventing unauthorised access to a host computer system”); EX1008, Abstract (“method for obtaining at least one item of user specific data, wherein the user specific data is obtained at least partly by using paging or a short message service”) EX1003, ¶¶69, 118.

In addition, each of these references is reasonably pertinent to at least one problem that would have concerned the inventor of the '658 Patent, *e.g.*, that user authentication “could be achieved using a device that many users already carry-a personal communication device such as a mobile phone or a pager.” EX1001, 1:56-59. Likewise, *Veneklase* solves the same problem using a generated random code sent to the user’s conventional and commercially available pager. *See, e.g.*, EX1005,

8:5-15. Similarly, *Jonsson* solves the problem of prior art systems “require[ing] specially equipped, and often dedicated, terminals, which raises the cost and reduces the availability of the associated electronic service.” *See, e.g.*, EX1006, 2:8-14. *Kew* solves the same problem using a generated random code sent “in a fashion similar to conventional paging systems.” *See, e.g.*, EX1005, 8:15-19. *Sormunen* solves that problem by sending authentication information to the user via a mobile network. *See, e.g.*, EX1006, 4:30-5:8; EX1003, ¶¶70, 119.

IV. MANDATORY NOTICES

A. Real Party-in-Interest

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies that Unified is the real party-in-interest, and further certifies that no other party exercised control or could exercise control over Unified’s participation in this proceeding, the filing of this petition, or the conduct of any ensuing trial. In view of *Worlds Inc. v. Bungie, Inc.*, 903 F.3d 1237, 1242-44 (Fed. Cir. 2018), Unified has submitted voluntary discovery in support of its certification. *See* EX1014 (Declaration of Kevin Jakel).

B. Related Matters

According to USPTO records, the ’658 Patent is assigned to Dynapass IP Holdings LLC. Petitioner is aware of the following litigation asserting the ’658 Patent:

- *Dynapass IP Holdings LLC v. Regions Financial Corporation et al*, 2:22-cv-00215 (EDTX 6-17-2022);
- *Dynapass IP Holdings LLC v. JPMorgan Chase & Co. et al*, 2:22-cv-00212 (EDTX 6-17-2022);
- *Dynapass IP Holdings LLC v. PlainsCapital Bank et al*, 2:22-cv-00213 (EDTX 6-17-2022);
- *Dynapass IP Holdings LLC v. Woodforest National Bank et al*, 2:22-cv-00218 (EDTX 6-17-2022);
- *Dynapass IP Holdings LLC v. Bank of America Corporation et al*, 2:22-cv-00210 (EDTX 6-17-2022);
- *Dynapass IP Holdings LLC v. Wells Fargo & Company et al*, 2:22-cv-00217 (EDTX 6-17-2022);
- *Dynapass IP Holdings LLC v. Truist Financial Corporation et al*, 2:22-cv-00216 (EDTX 6-17-2022);
- *Dynapass IP Holdings LLC v. PNC Financial Services et al*, 2:22-cv-00214 (EDTX 6-17-2022);
- *Dynapass IP Holdings LLC v. BOKF, National Association et al*, 2:22-cv-00211 (EDTX 6-17-2022);

- *Dynapass Inc. v. Mobile Authentication Corporation et al*, 8:18-cv-01173 (C.D. Cal. 7-3-2018).

C. Petitioner is aware that the '658 Patent has been challenged in IPR2023-00367 on January 3, 2022.**Lead and Back-up Counsel**

Lead Counsel: Jordan M. Rossen (Reg. No. 74,064)

Back-up Counsel: Ashraf Fawzy (Reg. No. 67,914)

D. Service Information, Email, Hand Delivery, and Postal

Unified consents to electronic service at jordan@unifiedpatents.com and afawzy@unifiedpatents.com. Petitioner can be reached at Unified Patents, LLC, 4445 Willard Ave., Suite 600, Chevy Chase, MD, 20815, (202) 701-1850.

V. CERTIFICATION OF GROUNDS FOR STANDING

Petitioner certifies pursuant to Rule 42.104(a) that the patent for which review is sought is available for *inter partes* review and Petitioner is not barred or estopped from requesting an *inter partes* review challenging the patent claims on the grounds identified in this Petition.

VI. DISCRETIONARY INSTITUTION

The Board should not exercise its discretion under either 35 U.S.C. §§ 314(a) or 325(d) to deny this Petition.

The '658 Patent was challenged on January 3, 2022, three days before this filing. Unified first learned about it after it was filed, through publicly available

information (i.e., public docket filings).

General Plastic (“GP”) factor one (extended in *Valve*) weighs against discretionary denial. *Valve v. Electronic Scripting*, IPR2019-00062, Paper 11 (Apr. 2, 2019) (precedential) (“*Valve*”). Unified did not coordinate the IPR2023-00367 petition. Unified and the petitioners in IPR2023-00367 have no *Valve*-like “significant relationship.” Unified has acted diligently to prepare this Petition independently and filed long before any response in IPR2023-00367. *Mercedes-Benz v. Carucel*, IPR2019-01404, Paper 12, 13-14 (Jan. 22, 2020) (finding these facts weighed against discretionary denial under Factors 2-7).

Material differences in the petitions favor institution. Unified is not a defendant in any litigation and challenges different claims than IPR2023-00367, including claim 4. Unified bases its Petition on two separate grounds, only one of which has a single secondary reference in common with IPR2023-00367. *Xilinx v. Arbor Global Strategies*, IPR2020-01568, Paper 12, 10-12 (Mar. 5, 2021) (GP analysis weighed against discretionary denial where later petition challenged additional claims and its grounds presented “materially different challenges”). As noted below, Unified does not rely on any reference considered during prosecution.

To the best of Petitioner’s knowledge, Patent Owner has asserted the ’658 Patent in ten district court litigations. *See* Section IV.

In *Apple Inc. v. Fintiv, Inc.*, the Board set forth six factors guiding the exercise

of discretion under § 314(a) by considering efficiency, fairness, and the merits in view of an earlier trial date. IPR2020-00019, Paper 11 (3-20-2020) (precedential). The *Fintiv* factors weigh in favor of institution.

Fintiv factor 1 favors institution or is at least neutral, as Unified is not a participant to any proceedings involving the '658 Patent, so no stays would be necessary. Further, none of the parties had any prior knowledge about this Petition and Petitioner is not in communication with them. Jakel Decl. (EX1017).

Fintiv factor 2 favors institution, as Unified is not a participant in any cases involving the '658 Patent and the trial date is set for April 15, 2024. Further, whether these trials will proceed at all, let alone as scheduled, is speculative at best.

Fintiv factor 3 favors institution, as Petitioner is not a party to any litigation involving the '658 Patent and, therefore, has not expended resources in that litigation. Further, Unified does not have any knowledge of resources expended by the parties in the parallel district court litigation other than public information, but it appears that these litigations are still in their early stages and no investment has been made with respect to the merits of invalidity.

Fintiv factor 4 favors institution, as there is minimal overlap. Petitioner has filed this IPR due to its unique business model of deterring non-practicing entities from asserting patents of poor quality against strategic technologies and industries. See, e.g., Jakel Decl. (EX1017), ¶¶2-3. As Petitioner's perspective, goals and

business model is unique, it has independently pursued invalidity grounds, prior art and claim selection without discussion, interaction, involvement, or input of any kind with any defendant. *Id.*, ¶¶4-5, 13. This Petition challenges claims 1, 3-6, while only claim 5 is asserted in the district court cases. Thus, the district court will leave at least one of the Challenged Claims unchallenged.

Fintiv factor 5 weighs heavily against discretionary denial. Petitioner is not a defendant in the district court case, is not a real party-in-interest, or in privity with the defendants.

Finally, *Fintiv* factor 6 strongly weighs against discretionary denial. The merits of the Petition are extremely strong. *Fintiv*, Paper 11, 14-15. For example, the Petition demonstrates—in two separate grounds—that the prior art discloses every limitation in each of the Challenged Claims. Section III.

Thus, when considering all the *Fintiv* factors, the factors weigh heavily against discretionary denial. Declining to institute this Petition as a result of parallel litigation, in which Petitioner is not involved, would only serve to permit further assertion of an invalid patent rather than serving Congress’s stated purpose in re-evaluating patents that never should have issued in the first place.

Further, *Veneklase*, *Jonsson*, *Kew*, and *Sormunen* were not cited during examination, and there is no “overlap between the arguments made during examination and the manner in which Petitioner relies on the prior art.” *Becton*,

Dickinson & Co. v. B. Braun Melsungen AG, IPR2017-01586, Paper 8, 17-18 (12-15-2017) (precedential). Only *Sormunen* is relied on in IPR2023-00367 and it was a secondary reference combined with an entirely different primary reference. Therefore, under the first part of the *Advanced Bionics* framework, the Board should not exercise its discretion to deny institution under § 325(d). *Adv. Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6, 8-9 (2-13-2020) (precedential). Under the second part, the Office erred in allowing the Challenged Claims because they are rendered obvious (1) by *Veneklase* and *Jonsson* and (2) by *Kew* and *Sormunen* for the reasons presented in Section III.

VII. CONCLUSION

For the foregoing reasons, Petitioner requests IPR of the Challenged Claims of the '658 Patent.

Dated: January 6, 2023

Respectfully Submitted,

/Jordan M. Rossen /

Jordan M. Rossen

Registration No. 74,064

Ashraf Fawzy

Registration No. 67,914

CERTIFICATION UNDER 37 CFR § 42.24(d)

Under the provisions of 37 CFR §42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review—excluding the Table of Contents, List of Exhibits, Mandatory Notices, Certification Under § 42.24(d), and Certificate of Service—totals 13,860 words, which is less than the 14,000 allowed under 37 CFR §42.24(a)(i).

Dated: January 6, 2023

Respectfully Submitted,

/Jordan M. Rossen /
Jordan M. Rossen
Registration No. 74,064

Unified Patents, LLC

4445 Willard Ave., Suite 600
Chevy Chase, MD, 20815
Tel: (202) 701-1850

CERTIFICATE OF SERVICE

I hereby certify that on January 6, 2023, I caused true and correct copies of the foregoing **Petition for *Inter Partes* Review for U.S. Patent No. 6,993,658, Power of Attorney, and Exhibits 1001 through 1017** to be served via Priority Mail Express Delivery on the following counsel of record for the subject patent:

Jerry Swell, Esq.
DynaPass Inc.
P.O. Box 11510
Costa Mesa, CA 92627

Dated: January 6, 2023

By: /Ashley F. Cheung/
Ashley F. Cheung
Paralegal
Unified Patents, LLC