

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, LLC
Petitioner

v.

DYNAPASS IP HOLDINGS LLC
Patent Owner

Case No. IPR2023-00425
U.S. Patent 6,993,658

DECLARATION OF BRUCE MCNAIR

Table of Contents

I.	Background and Qualifications	5
II.	Legal Framework.....	8
A.	Obviousness.....	8
i.	General Framework	9
ii.	Analogous Art	10
iii.	Combining Known Elements in the Art, Common Sense.....	11
iv.	Teaching Away.....	14
v.	Secondary Considerations	14
B.	Claim Construction.....	16
i.	“Cell phone network”	17
ii.	“Not known to the user”	17
iii.	“a control module...configured to...”; “a communication module configured to...”; “an authentication module configured to...”	20
i.	“a control module...configured to”	21
ii.	“a communication module configured to”	21
iii.	“an authentication module configured to”.....	21
III.	Summary of my Opinions.....	22
IV.	Technical Background.....	23
A.	Security services.....	23
B.	Authentication techniques	26
i.	Passwords	26
ii.	Challenge response	27

iii.	One time passwords.....	29
iv.	Multifactor authentication	30
v.	Smart cards	31
C.	Time-bound access	32
V.	Level of Skill of a Person Having Ordinary Skill in the Art	33
VI.	Overview of U.S. Patent No. 6,993,658	34
A.	Prosecution History	39
VII.	Grounds of Unpatentability	41
A.	Ground 1: Claim 5 Is Obvious over <i>Veneklase</i> in view of <i>Jonsson</i> 41	
i.	Overview of <i>Veneklase</i>	41
ii.	Overview of <i>Jonsson</i>	43
iii.	Analogous Art	45
iv.	Claim 5	46
	Motivations to Combine <i>Veneklase</i> and <i>Jonsson</i>	60
B.	Ground 2: Claims 1 and 3-6 Are Obvious over <i>Kew</i> in view of <i>Sormunen</i>	75
i.	Overview of <i>Kew</i>	75
ii.	Overview of <i>Sormunen</i>	78
iii.	Analogous Art	79
iv.	Claim 5	80
	Motivations to Combine <i>Kew</i> and <i>Sormunen</i>	89
v.	Claim 6	104
vi.	Claim 1	105
vii.	Claim 3	109

viii. Claim 4	111
VIII. Conclusion	112

I. BACKGROUND AND QUALIFICATIONS

1. My name is Bruce McNair, and I am over 21 years old and otherwise competent to make this Declaration. I make this Declaration based on facts and matters within my own knowledge and on information provided to me by others, and, if called as a witness, I could and would competently testify to the matters set forth herein.

2. I have been retained as a technical expert witness in this matter by Counsel for the Petitioner, Unified Patents, LLC (“Petitioner”) to provide my independent opinions on certain issues requested by Counsel for Petitioner relating to the accompanying Petition for *Inter Partes* Review of U.S. Patent No. 6,993,658 (“the ’658 Patent”), challenging Claims 1 and 3-6 (the “Challenged Claims”). My compensation in this matter is not based on the substance of my opinions or on the outcome of this matter. I have been informed that Dynapass IP Holdings LLC (“Patent Owner”) is the purported owner of the ’658 Patent. I note that I have no financial interest in Petitioner or Patent Owner, and I have no other interest in the outcome of this matter.

3. I received my Bachelors of Engineering and Masters of Engineering - Electrical Engineering from the Stevens Institute of Technology in 1971 and 1974, respectively. I also completed qualifiers and course work for a Ph.D. in computer science.

4. I have over 55 years of industry experience in the areas of electronic circuits, including substantial time spent working with voice-input technology. Starting in 1963, I worked as an amateur radio operator in 1963. My experience includes seven years as a GS-0855 Electronic Engineer working for the US Army Electronics Command, 24 years as a Member of Technical Staff at AT&T/Bell Laboratories and 15 years as a full-time faculty member of the Electrical and Computer Engineering Department at Stevens Institute of Technology.

5. While I was working for the US Army Electronics Command at Fort Monmouth, NJ, I was responsible for support of TSEC/KG-27 bulk encryptor, a classified encryption device used by the Army for protecting multi-channel digital voice communications lines. Also, while I was at Fort Monmouth, my responsibilities included research and development for the cryptographic aspects of SINCGARS, the Single Channel Ground/Airborne Radio System.

6. During my employment at AT&T/Bell Labs, in the early 1980s, I worked closely with the Acoustics and Speech Processing Research Department and used their research to implement low-bit rate speech coding for a secure voice terminal. Later, in the mid-1980s, I managed a group that designed speech processing for speaker verification and natural language speech recognition. As part of this work, I used the AT&T 3450 cellular telephone which employed voice dialing. I also initiated and led an IR&D (independent research and development)

project to investigate and prototype a secure voice terminal based on newly evolving AT&T high-speed digital services.

7. From 1987 until 1994, I led the AT&T Bell Labs Security and System Reliability Architecture Group. In the course of this activity, I investigated security in all aspects of AT&T products and services. I also led efforts to employ the newly developed AT&T Smart Card as a personal authenticator for use in the AT&T networks operations centers.

8. I am named on multiple domestic and international patents related to encryption devices, voice-based security systems, and network security.

9. As part of my work in forming my opinions in connection with this proceeding, I have reviewed the following materials, which I believe those in the field would reasonably rely upon in forming opinions regarding the subject matter of this proceeding:

Exhibit No.	Description
1001	U.S. Patent 6,993,658
1002	Prosecution History File of Application 09/519,829
1005	European Patent Application No. 084451 to Veneklasé (“ <i>Veneklasé</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

	("Sormunen")
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

II. LEGAL FRAMEWORK

A. Obviousness

10. I am a technical expert and do not offer any legal opinions. However, I have been informed about certain legal principles regarding patentability and related matters under United States patent law, which I have applied in performing my

JPMORGAN EXHIBIT 1003

analysis and arriving at my technical opinions in this matter.

i. General Framework

11. I am informed that a person cannot obtain a patent on an invention if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious to a person having ordinary skill in the art obvious at the time of the invention. I am informed that a conclusion of obviousness may be founded upon more than a single item of prior art. I am also informed that obviousness is determined by evaluating the following factors: (1) the scope and content of the prior art, (2) the differences between the prior art and the claim at issue, (3) the level of ordinary skill in the pertinent art, and (4) secondary considerations of non-obviousness. In addition, the obviousness inquiry should not be done in hindsight. Instead, the obviousness inquiry should be done through the eyes of a person having ordinary skill in the art at the time of the alleged invention.

12. In considering whether certain prior art renders a particular patent claim obvious, I am informed that one must consider the scope and content of the prior art, examples of which include disclosures in patents, trade publications, journal articles, conference papers, industry standards, product literature and documentation, texts describing competitive technologies, requests for comment published by standard setting organizations, and materials from industry conferences.

13. I am informed that for a patent claim to be found obvious, the proper

perspective to consider is that of a person having ordinary skill in the art (often referred to as a “PHOSITA,” “POSITA,” or “POSA”) at the time of the alleged invention. I am informed that the factors to consider in determining the level of ordinary skill in the art include (1) the educational level and experience of people working in the field at the time the invention was made, (2) the types of problems faced in the art and the solutions found to those problems, and (3) the sophistication of the technology in the field.

ii. Analogous Art

14. I am informed that for a prior art reference to be proper for use in an obviousness analysis, the reference must be “analogous art” to the claimed invention. I am informed that a reference is analogous art to the claimed invention if: (1) the reference is from the same field of endeavor as the claimed invention (even if it addresses a different problem); or (2) the reference is reasonably pertinent to the problem faced by the inventor (even if it is not in the same field of endeavor as the claimed invention). In order for a reference to be “reasonably pertinent” to the problem, it must logically have commended itself to an inventor's attention in considering his problem. In determining whether a reference is reasonably pertinent, one should consider the problem(s) faced by the inventor, as reflected either explicitly or implicitly, in the specification. Such problems are not limited to those solved by the purported invention, but the general problem(s) that confronted the

inventor before the invention was made. I believe that all of the references I considered in forming my opinions in this IPR are well within the range of references a person having ordinary skill in the art would have consulted by the time of the invention to address the type of problems described in the Challenged Claims.

iii. Combining Known Elements in the Art, Common Sense

15. I am informed that, in order to establish that a claimed invention was obvious based on a combination of prior art elements, a clear articulation of the reason(s) why a claimed invention would have been obvious must be provided. Specifically, I am informed that, under the U.S. Supreme Court's KSR decision, a combination of multiple items of prior art renders a patent claim obvious when there was an apparent reason for a person having ordinary skill at the time of the invention to combine or modify the prior art. I am informed that such reason may include, but is not limited to, one or more of the following rationales: (A) combining prior art methods according to known methods to yield predictable results; (B) substituting one known element for another to obtain predictable results; (C) using a known technique to improve a similar device in the same way; (D) applying a known technique to a known device ready for improvement to yield predictable results; (E) trying a finite number of identified, predictable potential solutions, with a reasonable expectation of success; (F) identifying that known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based

on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art; or (G) identifying an explicit teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine the prior art references to arrive at the claimed invention.

16. I am informed that the test for obviousness is not whether the features of a secondary reference may be *bodily incorporated* into the structure of the primary reference, but rather whether one of skill would have been motivated to combine the teachings of the prior art references to achieve the claimed invention. Nevertheless, I am informed that an invention that is a combination of prior art must do more than yield predictable results to be non-obvious and that, even where one or more motivations to combine exist, claims are not necessarily obvious unless a person having ordinary skill in the art would have had a reasonable expectation of success in implementing or applying the proposed combination at the time of the invention.

17. I also am informed that in conducting an obviousness analysis, a precise teaching directed to the specific subject matter of the challenged claim need not be sought out because it is appropriate to take account of the inferences and creative steps that a person having ordinary skill in the art at the time of the invention would employ. In other words, the prior art need not be directed towards solving the same specific problem as the problem addressed by the patent. Further, the individual prior

art references themselves need not all be directed towards solving the same problem. The prior art considered can be directed to any need or problem known in the field of endeavor at the time of invention and can provide a reason for combining the elements of the prior art in the manner claimed. Common sense teaches that familiar items may have obvious uses beyond their primary purposes, and a person having ordinary skill in the art will often have been able to fit the teachings of multiple prior art references like pieces of a puzzle. I am informed that, under the *KSR* standard, common sense is important and should be considered in assessing obviousness.

18. I also am informed that the fact that a particular combination of prior art elements was “obvious to try” may indicate that the combination was obvious even if no one attempted the combination. If the combination was obvious to try (regardless of whether it was actually tried) or leads to anticipated success, then it is likely the result of ordinary skill and common sense rather than innovation. I am further informed that in many fields it may be that there is little discussion of obvious techniques or combinations, and it often may be the case that market demand, rather than scientific literature or knowledge, will drive the design of an innovation. When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person having ordinary skill in the art has good reason to pursue the known options within his or her technical grasp. If this leads to the anticipated success, it is likely the product not of innovation, but of

ordinary skill and common sense.

iv. Teaching Away

19. I am informed that it is improper to combine references where the references teach away from their combination. I am informed that a reference may be said to teach away when a person of skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the patent applicant. In general, a reference will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the patentee. I am informed that a reference teaches away, for example, if (1) the combination would produce a seemingly inoperative device, or (2) the references leave the impression that the product would not have the property sought by the patentee. However, I am informed that a reference does not teach away if it merely expresses a general preference for an alternative invention but does not criticize, discredit, or otherwise discourage investigation into the invention claimed. Further, a person of skill will often appreciate that different courses of action often have simultaneous advantages and disadvantages, and I am informed the existence of such does not necessarily obviate a motivation to combine.

v. Secondary Considerations

20. I am informed that even if a *prima facie* case of obviousness is

established, the final determination of obviousness must also consider “secondary considerations” if presented. I am informed that in most instances, the patentee raises these secondary considerations of non-obviousness. In that context, the patentee argues an invention would not have been obvious in view of these considerations, which include: (a) commercial success of a product due to the merits of the claimed invention; (b) a long-felt, but unsatisfied need for the invention; (c) failure of others to find the solution provided by the claimed invention; (d) deliberate copying of the invention by others; (e) unexpected results achieved by the invention; (f) praise of the invention by others skilled in the art; (g) lack of independent simultaneous invention within a comparatively short space of time; (h) teaching away from the invention in the prior art.

21. I am further informed that secondary-considerations evidence is only relevant if the offering party establishes a connection, or nexus, between the evidence and the claimed invention. The nexus cannot be based on prior art features. For example, if commercial success of products allegedly embodying the claims is presented as a secondary indicium of non-obviousness, the patent owner must show that such success is due to features of the claimed invention, and not features unrelated to the claimed invention or that already existed in the prior art. The establishment of a nexus is a question of fact. While I understand that the Patent Owner here has not offered any secondary considerations at this time, I will

supplement my opinions in the event that Patent Owner raises secondary considerations during the course of this proceeding.

B. Claim Construction

22. I am informed that in performing an obviousness analysis, it is necessary to understand the scope of the claims. I am also informed the first step in an unpatentability analysis, therefore, involves construing the claims. Second, the construed claim language is then compared to the disclosures of the prior art.

23. I am informed that claims are generally given their ordinary and custom meaning as understood by one of ordinary skill in the art at the time of the invention, in light of the patent specification. I am informed that, for the purposes of claim construction, expert testimony may be helpful to provide background on the technology at issue, to explain how an invention works, to ensure an understanding of the technical aspects of the patent is consistent with that of a person having ordinary skill in the art, or to establish that a particular term in the patent had a particular meaning in the pertinent field at the time of the invention. However, I am also informed testimony from a technical expert is generally less reliable than the patent itself and its prosecution history in determining the meaning of claim terms, and it is not the role of technical experts to supplant courts and PTAB judges in applying principles of claim interpretation.

24. For the purposes of my analysis below, I have reviewed the claim

language, the specification, and the prosecution history. For the purposes of my analysis below, I do not believe that any of the claim terms require a specific construction beyond the plain and ordinary meaning as would be understood by a POSITA. That being said, I address certain claim terms below.

i. “Cell phone network”

25. 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. In addition, claim 4 of the ’658 Patent, which, depends from claim 1, requires that “the personal communication device is a pager.” EX1001, 12:18-19. Thus, it is my opinion that 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.

ii. “Not known to the user”

26. 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.” 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. 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

27. 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. This is confirmed by the '658 Patent's specification, which describes "information provided to the user through an object possessed by the user, such as the token." *Id.*, 2:11-15.

28. Thus, it is my opinion that 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.

iii. "a control module...configured to..."; "a communication module configured to..."; "an authentication module configured to..."

29. I have been told that there is special rule for construing means-plus-function limitations that involves two steps: (1) identifying the claimed function, and (2) determining what structure corresponds to that claimed function. I have been informed that the claim terms "control module...configured to," "communication module configured to," and "authentication module configured to" may be considered as means-plus-function limitations. While I provide no opinion as to whether those terms are means-plus-function terms, I have been asked to consider the function and the structure as disclosed in the '658 Patent for these claim terms as

they would have been understood by a person of ordinary skill in the art.

i. “a control module...configured to”

30. 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 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.

ii. “a communication module configured to”

31. 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.

iii. “an authentication module configured to”

32. 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.

III. SUMMARY OF MY OPINIONS

33. In my opinion, claims 1 and 3-6 of the '658 Patent are unpatentable, based on my review of the '658 Patent, the file history of the '658 Patent, the scope of the prior art discussed in the Petition, the knowledge and skill a person of ordinary skill in the art would have had by the time of the '658 Patent, and additional background materials discussed below. If the Patent Owner submits additional evidence pertaining to the patentability of the '658 Patent, I intend to review such materials and update my analysis and conclusions as appropriate and as permitted under the rules of this proceeding.

34. I have also relied on my education, experience, and knowledge in the

relevant field of art in forming my opinions expressed below.

IV. TECHNICAL BACKGROUND

A. Security services

35. The broad topic of security, as it is applied to computer and communication networks, can be discussed in terms of the various services that can be provided. The International Organization for Standardization (ISO) first published a standard in 1989, ISO 7498-2:1989 “Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture” that defines a set of six security services. The security services defined in this standard are:

- a. Identification – means to uniquely name and identify an entity
- b. Authentication – means to ensure the identified entity is who or what they claim to be
- c. Access Control – means to restrict access to only those system resources the entity is authorized to access
- d. Confidentiality – means to ensure information cannot be disclosed to an unauthorized party
- e. Integrity – means to ensure information cannot be accidentally or intentionally modified or damaged
- f. Non-repudiation – means to ensure that a party cannot deny having

engaged in a prior transaction.

36. While supervising the Bell Labs Security and System Reliability Architecture group from 1987 to 1994, I identified the need for a standard structure for discussing system security and realized that ISO 7498-2 addressed most, but not all, security issues. Notably, since it was created with computer systems in mind, it did not address issues a network service provider or military customer might find important, that is the Availability of service, which would address continuity of service in the presence of, for instance, denial of service attacks. Also, 7498-2 did not provide any structure to understand the interrelationship of these services. I enhanced the standard's model by adding the Availability service, and identified a structure to show all the services were interrelated. This model is illustrated in the figure below.

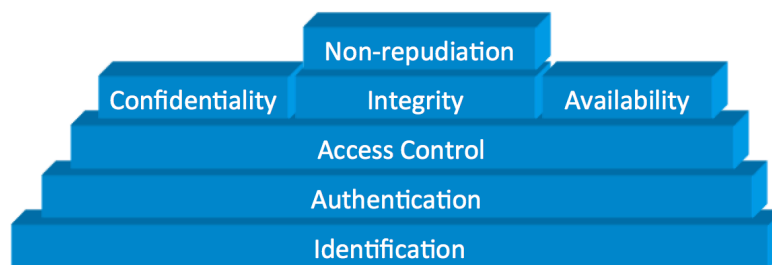


Figure 1 - Security service structure

37. As Figure 1 shows, Identification provides the basis for all other security services. One cannot reason about the security of a system without attributing actions to a specific entity. Authentication builds on Identification,

allowing the system to verify the individual or entity's identity. With their identity established and authenticated, it is now possible to determine what system resources they may access through Access Control services. Further building on the foundation of these fundamental, underlying services, one can reason about all of the higher level services, as described above. One important relationship that should be noted is that between Integrity and Non-Repudiation. While the Integrity service ensures the correctness of information, the Non-Repudiation service ensures that an individual cannot deny having engaged in a transaction. Clearly, it does not make sense to enforce a transaction unless it is possible to first ensure that the transaction is actually what it seems to be. By physical analogy, we can notarize duplicate copies of documents to ensure the parties will be bound to their agreements, but it would not make sense to do so if the contracts were written in pencil, allowing modification. Besides using this model in AT&T and Bell Labs products and services and sharing it with government and commercial customers starting in 1987, I have also presented this model at IEEE talks and have used it in my graduate security courses for over twenty years. *See, e.g., Invited talk: "Is Wireless Security an Oxymoron?," IEEE Princeton/Central NJ Communications and Consumer Electronics and Computer Science Chapters, December 16, 2003, accessible via the Rutgers/WINLAB YouTube channel.* I present it here to illustrate what the underlying structure of the broad term "security" can convey.

B. Authentication techniques

38. As described above, it is not sufficient to merely identify a person or entity using a system. To ensure system security, there must be a means to ensure proof of an identity claim, which is the intent of authentication. There have historically been numerous ways to authenticate users or computer processes using services and the sections below present several security mechanisms that can provide authentication.

39. In order to communicate securely, it is necessary for a user or client device to make an identity claim to a server or network resource in order to determine to what access should be granted. By way of analogy, only someone with a valid account at a financial institution should be able to write a check. Since anyone can make an identity claim, the necessary second step is to provide some means to validate that claim. Fundamentally, the purpose of authentication is to validate identity claims. Continuing the check-writing analogy, a check is validated by requiring an authorized signature (Authentication) and contains a number of printed features to prevent unauthorized alteration (Integrity).

i. Passwords

40. Simple user IDs and passwords or PINs have been used for several decades to identify users and authenticate their identity under the theory that only the user has knowledge of the password or PIN. Of course, one inherent flaw in

such systems is that during the process of providing identification and authentication, the user could be compromised if, for example, the server is itself compromised or if the attacker is monitoring the communications channel. One famous example of the latter situation is given in the 18th-century story “Ali Baba and the Forty Thieves” where Ali Baba overhears the authentication phase “Open Sesame” and later uses it to gain unauthorized access to the thieves’ lair. Unfortunately, “sesame” has been one of the most used passwords in computer system as is “password.”

41. Numerous studies have shown that humans tend to use PINs and passwords that are easy to predict (e.g., children’s names, birthdates, etc.) or can be found in a dictionary. EX1009, 24-29. Thus, system generated passwords that users will, unfortunately, have difficulty remembering or complex restrictions on allowable passwords (e.g., mixed letter case, number, special character requirements) are mandated to attempt to improve security. Faced with the conflicting problems of passwords that are easy to remember but are not subject to guessing or dictionary search, alternatives to simple passwords have long been considered to improve authentication security.

ii. Challenge response

42. Challenge-response systems are another means to authenticate a user to ensure they are who they claim to be. The trivial challenge-response system is

actually just a basic password or personal identification number (PIN) system. The challenge is the request for a PIN or password and the response is the PIN or password. The limitation of these basic challenge-response systems is that an eavesdropper listening to the exchange can record the PIN or password and use it as a later time to masquerade as the intended authorized user.

43. One way to overcome the problem of monitoring is by the use of encryption where the authentication phrase is enciphered. One of the earliest computer systems to use PINs for authentication was the Atalla box, a hardware security module which launched in 1973 and quickly gained popularity for use with ATMs. The Atalla box, which is patented in U.S. Patent No. 3,938,091, did not directly send user PINs but rather first encrypted a user's PIN and sent the encrypted PIN to a, for example, bank teller. EX1010. The teller would then confirm the authenticity of the PIN by encrypting the teller's copy of the user's PIN and comparing the output with the received encoded PIN.

44. However, if encryption uses a symmetric cryptosystem where the message is encrypted and decrypted with the same shared key, prior arrangement to distribute the encryption key between the parties is needed. One way would be for the user to share its secret key with every server it may wish to access, but such a method can be cumbersome and vulnerable to attack. An alternative method is the use of trusted key distribution servers which, if properly designed, may overcome

the issue of the unauthorized third-party monitoring communications. One such system is the Kerberos system which was first used by MIT for their Project Athena local network in the early 1980s. Kerberos v4 was widely distributed for public use in the late 1980s and Kerberos v5 became an Internet standard in 1993 (RFC 1510).

45. While the initial versions of Kerberos were based on DES, by the mid-1990s, it was recognized that the rapid evolution of technology created vulnerabilities in DES and required its replacement. Moreover, Kerberos's use of symmetric encryption posed scalability and security problems, such as the centralized sever being a single point of failure, e.g. an attacker who compromised the server would have access to every secret key used by every single user. Several alternatives to DES, including public key cryptosystems, for use in Kerberos were introduced in the mid-1990s, such as SESAME V4 in 1995 and initial drafts of PKINIT (to later become RFC 4556) in 1997.

iii. One time passwords

46. As the name suggests, a one time password or "OTP" system uses passwords that are only used a single time. In this way, even if an attacker were able to monitor transmission of a password value, this particular password value would not be usable for subsequent interactions. There are many commercial instances of OTP systems, most notably RSA's SecurID. SecurID consists of a physical device with a Liquid Crystal Display (LCD) that shows a numeric value that changes every

60 seconds. Users who wish to authenticate themselves to a remote system must type in the value displayed on the LCD. The remote system has a locally generated numeric value to compare the entered value to and, if the two match, the user is authenticated. Besides SecurID, one time passwords systems may be based on the Internet Engineering Task Force (IETF)'s RFC2289. EX1011.

iv. Multifactor authentication

47. Multifactor authentication is a term used to indicate that more than one means of authentication may be used at a time. In general, authentication may be based on (a) what you know (e.g., a password), (b) what you have (e.g., a physical key, some sort of token, or an electronic device like a SecurID), (c) what you are (e.g., a biometric authenticator like, for instance, voice verification, retina scan, fingerprint, or handprint geometry), (d) where you are (e.g., geographic location, telephone number identification or Internet Protocol (IP) address), or (e) how you act (e.g., typing cadence or walking gait pattern). With multifactor authentication, two or more different authentication mechanism may be combined. The fundamental idea of multifactor authentication is that, while there will be an additive difficulty for a valid user to perform multiple authentication steps, the work effort is multiplicative for an attacker as he must tackle each gate separately. For instance, if authentication method A has a probability of falsely accepting an attacker of 5% and authentication method B has a probability of falsely accepting an attacker of

10%, the probability that an attacker will successfully pass both gates is 0.5% ($.05 \times .1 = .005$). Of course, this is a simplistic example. One would expect that each individual authentication method would be much harder than the example for an attacker to get through. Multifactor authentication is coming into widespread use today but was known and used by POSITAs more than 30 years ago.

v. **Smart cards**

48. In the past, credit cards depended solely on an embossed number containing the account number. This was replaced by magnetic stripe cards with the account number recorded digitally on the magnetic stripe, much as music could be recorded on a cassette audio tape. Unfortunately, this technique is equivalent to a simple password with no security protecting against monitoring or copying. Today, we use “chip” cards, a form of a smart card, but the original smart cards have been around since the 1960s. *See, e.g.,* DE1574074A1 to Helmut Groettrup, entitled “Anti-Counterfeiting Identification Switch”, available at <https://worldwide.espacenet.com/patent/search/family/007128903/publication/DE1574074A1?q=pn%3DDE1574074A1> While the original smart cards had simple electronic circuitry embedded in the card, later smart cards had full-blown computers, operating systems and secure file systems built into the card. EX1013. While at Bell Labs, I was involved in applying the AT&T Smart Card to secure the Network Operations Center where operators needed to manage multiple logins to

multiple network control systems, each requiring high levels of user authentication to assure secure network management. This replaced procedures where users needed to protect up to a dozen individual user IDs and passwords, which were sometimes written down and stored insecurely.

C. Time-bound access

49. The concept of time-bound access in secure systems is almost as old as the design of security systems. As an example, it is commonplace for systems that use cryptographic keys to “age” the keys as they are used. The principal reason for this is that the longer a cryptographic key is in use, the more information that depends on the security of that key will be transmitted and thus, the likelihood that an attacker will gain an advantage in breaking the security of a cryptosystem. In the worst case, if an encryption key is completely compromised, all the information transmitted using that encryption key will also be compromised. By restricting the time period for which the same cryptographic key is used, the loss of information can be mitigated. Also, in theoretical terms, any knowledge that an attacker may gain by acquiring encrypted information (ciphertext) and possibly obtaining or guessing corresponding information in its unencrypted form (plaintext) only increases as more information is sent using the same cryptographic key. From my experience with military cryptosystems in the 1970s, this resulted in military doctrine that required cryptographic keys be replaced periodically, known as the

“cryptoperiod,” even when doing so required onerous manual procedures to change encryption keys for a large number of terminals. EX1014. This concept has also been more broadly applied to system access and described in IEEE publications. EX1015, 1404-1408.

V. LEVEL OF SKILL OF A PERSON HAVING ORDINARY SKILL IN THE ART

50. I was asked to provide my opinion as to the level of skill of a person having ordinary skill in the field of the '658 Patent at the time of the claimed invention (referred to herein as a “POSITA”). I have been instructed to assume is that the time of the claimed invention of the '658 Patent is March 6, 2000. In determining the characteristics of a POSITA, I was told to consider several factors, including the type of problems encountered in the art, the solutions to those problems, the rapidity with which innovations are made in the field, the sophistication of the technology, and the education level of active workers in the field. I also placed myself back in the time frame of the claimed invention and considered the colleagues with whom I had worked at that time.

51. In my opinion, a POSITA would be a person having, as of March 6, 2000: at least (1) an undergraduate degree in electrical and computer engineering or a closely related field, such as physics or computer science, or similar advanced post-graduate education in this area; and (2) two or more years of experience in security,

with more experience substituting for less education and vice versa. Such a person of ordinary skill in the art would have been capable of understanding the '658 Patent and the prior art references discussed herein.

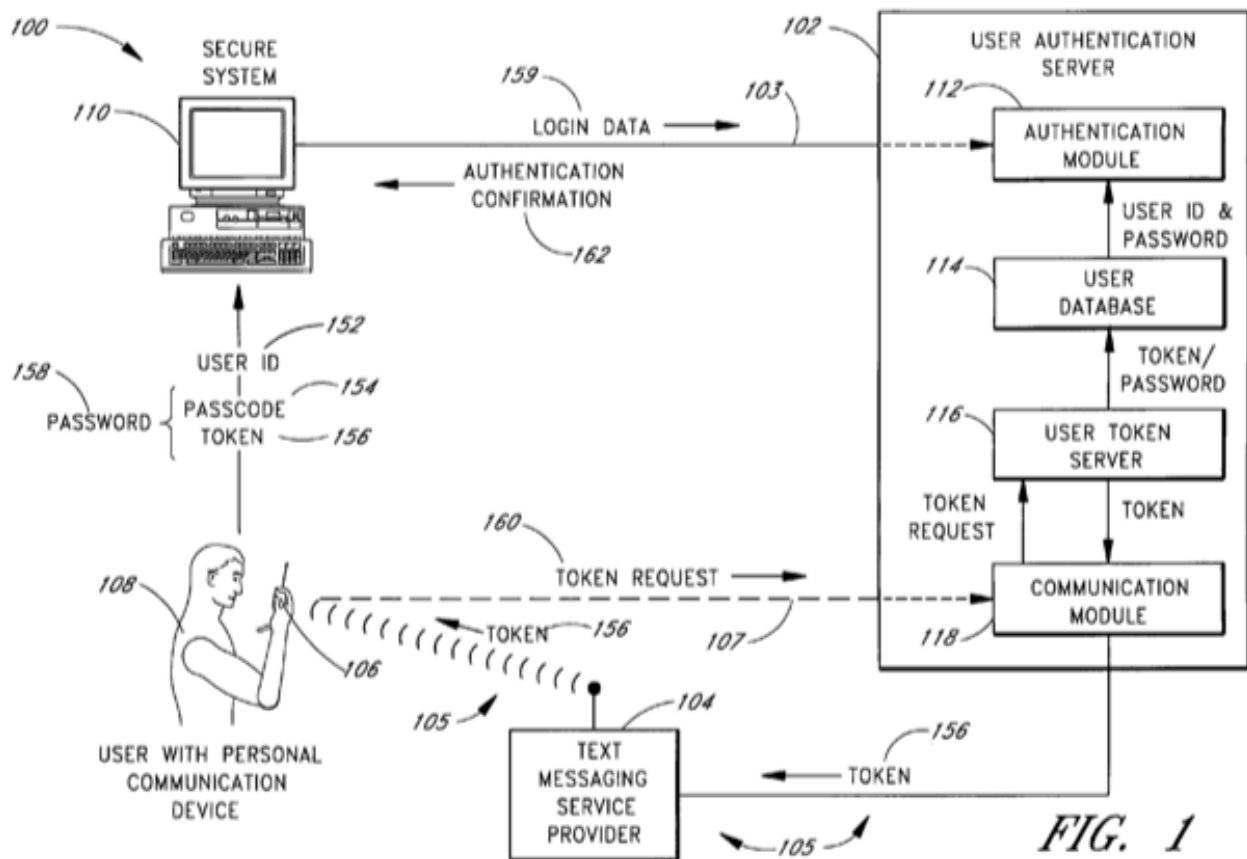
52. Based on my education, training, and professional experience in the field of the claimed invention, I am familiar with the level and abilities of a POSITA. Additionally, I met at least these minimum qualifications at least as of March 6, 2000. Further, although my qualifications may exceed those of the hypothetical person defined above, my analysis and opinions regarding the '658 Patent have been rendered from the perspective of a POSITA during the relevant time frame. In or before the relevant time frame, I had recruited and/or supervised persons having the stated level of experience.

VI. OVERVIEW OF U.S. PATENT NO. 6,993,658

53. 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.

54. 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 by combining the user’s passcode 154 ... with 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.

55. 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.

56. The '658 Patent has seven claims, including two independent claims. Independent Claim 5 is the broadest claim and recites the following:

- [5.0] A user authentication system comprising
- [5.1] a computer processor;
- [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;

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

57. Claim 6 depends from claim 5 and states:

- [6.0] The system of claim 5,
- [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.

58. Claim 1 is an independent claim and states:

- [1.0] A method of authenticating a user on a first Secure computer network, the user having a user account on Said first Secure computer network, the method comprising:
 - [1.1] associating the user with a personal communication device possessed by the user, said personal communication device in communication over a second network, wherein said second network is a cell phone network different from the first secure computer network;
 - [1.2] receiving a request from the user for a token via the personal communication device, over the second network;
 - [1.3] generating a new password for said first secure computer network based at least upon the token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user;
 - [1.4] setting a password associated with the user to be the new password;
 - [1.5] activating access the user account on the first secure computer network;
 - [1.6] transmitting the token to the personal communication device;
 - [1.7] receiving the password from the user via the first secure computer network; and
 - [1.8] 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.

59. Claim 3 depends from claim 1 and states:

[3.0] The method of claim 1,

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

60. Claim 4 depends from claim 1 and states:

[4.0] The method of claim 1,

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

A. Prosecution History

61. The '658 Patent was filed on March 6, 2000. On December 15, 2003, the Examiner rejected the pending claims as anticipated by Australia Patent Application No. 63545/98 from Schmitz or as obvious over that patent and Menezes. EX1002, 126-131. On March 11, 2004, Applicant responded by arguing that Schmitz did not disclose “receiving a request transmitted by the personal communication device,” which is a limitation found only in current claim 1, because it taught receiving the request from the data input apparatus and not the receiver. EX1002, 109-124. Applicant also argued 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. *Id.*

62. On May 24, 2004, the Examiner rejected the pending claims as

anticipated by Patent No. 5,323,146 to Glashick or Patent No. 6,226,364 to O'Neil, or obvious over the combination of the two. EX1002, 98-104. On August 26, 2004, Applicant responded by arguing that Glashick does not teach a personal communication device and instead only discloses a data station connected to the computer and by amending then claim 37, which was later cancelled. EX1002, 85-97. On February 7, 2005, the Examiner issued a final rejection maintaining its rejections because "Applicant's personal communication device, as viewed in light of Applicant's specification, is simply a type of computer with programs" and because "one skilled in the art would recognize that the motivation supplied by Glaschick would apply to *any* computerized system having authentication." EX1002, 72-80. On May 12, 2005, Applicant responded by filing an RCE and heavily amending the claims to require additional elements, including "said personal communication device configured to communicate over a cell phone network with the user authentication system" and the elements requiring the activation of access to the account in response to the password and deactivation of the account within a predetermined amount of time. EX1002, 59-64.

63. 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.

VII. GROUNDS OF UNPATENTABILITY

64. It is my opinion that claims 1 and 3-6 of the '658 Patent are unpatentable because they would have been obvious to a POSITA as of at least March 6, 2000, at least in light of the references discussed below and the knowledge and skill of a POSITA.

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

i. Overview of Veneklase

65. *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.

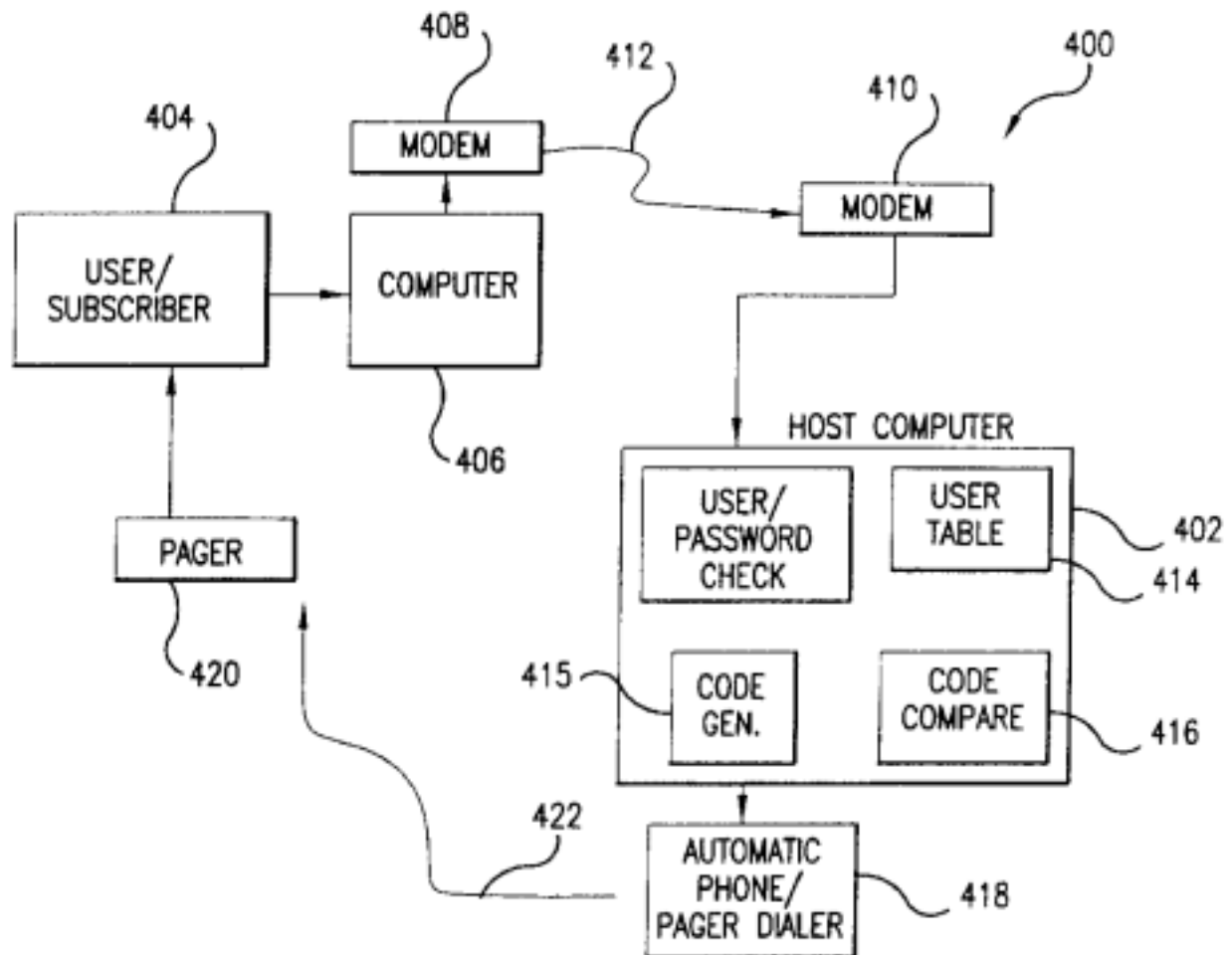


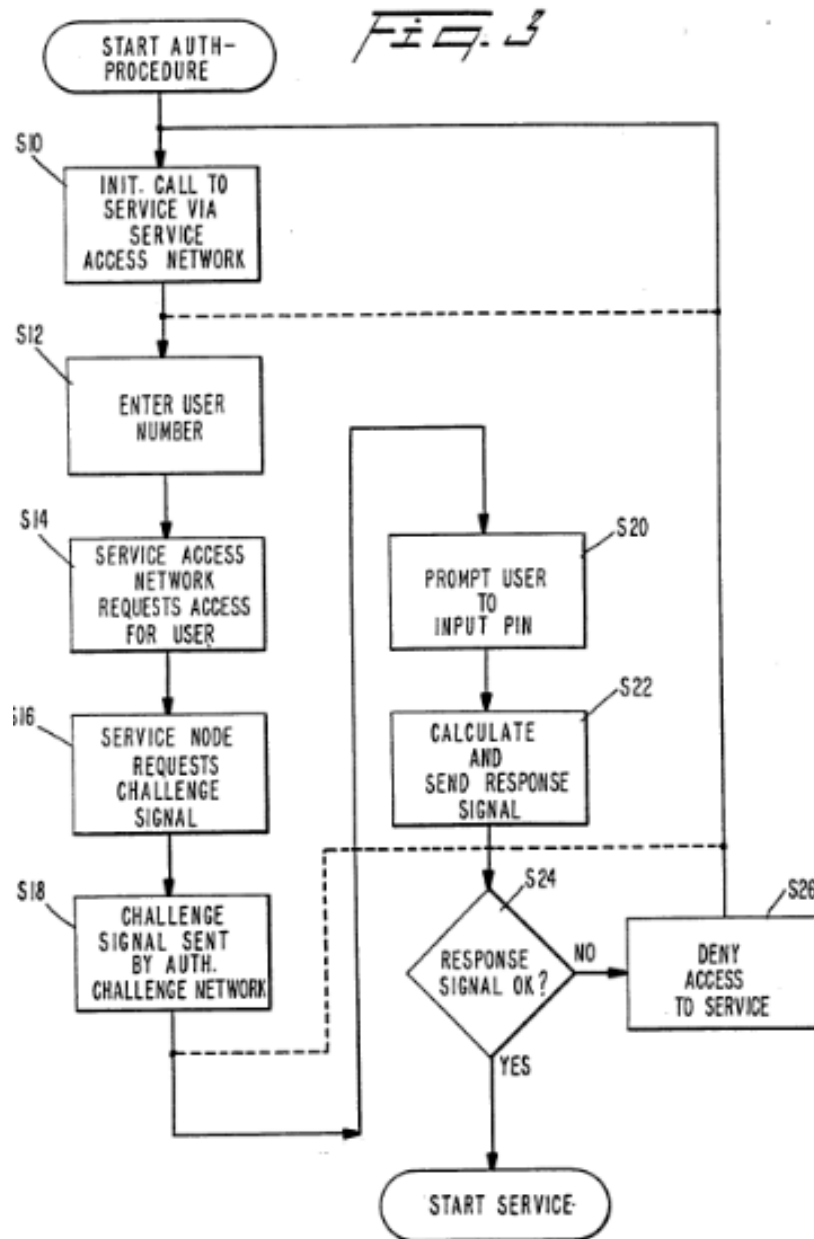
FIG.6

66. 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.

ii. Overview of Jonsson

67. *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.



68. 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.

iii. Analogous Art

69. *Veneklase* and *Jonsson* are analogous art. Both 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 (“relate[] 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.

70. In addition, each of these references is reasonably pertinent to at least one problem that would have concerned the inventor of the '658 Patent. *Id.* The

'658 Patent purported to solve the problem in which 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*’s system 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*’s system seeks to solve 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.

iv. Claim 5

[5.0] A user authentication system comprising

71. I have been informed by counsel that, as a matter of law, the preamble may or may not limit the scope of the claims. To the extent the preamble is deemed limiting, it is my opinion that a POSITA would have understood that *Veneklase* teaches this limitation; any alleged differences would have been obvious. *Veneklase* 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.

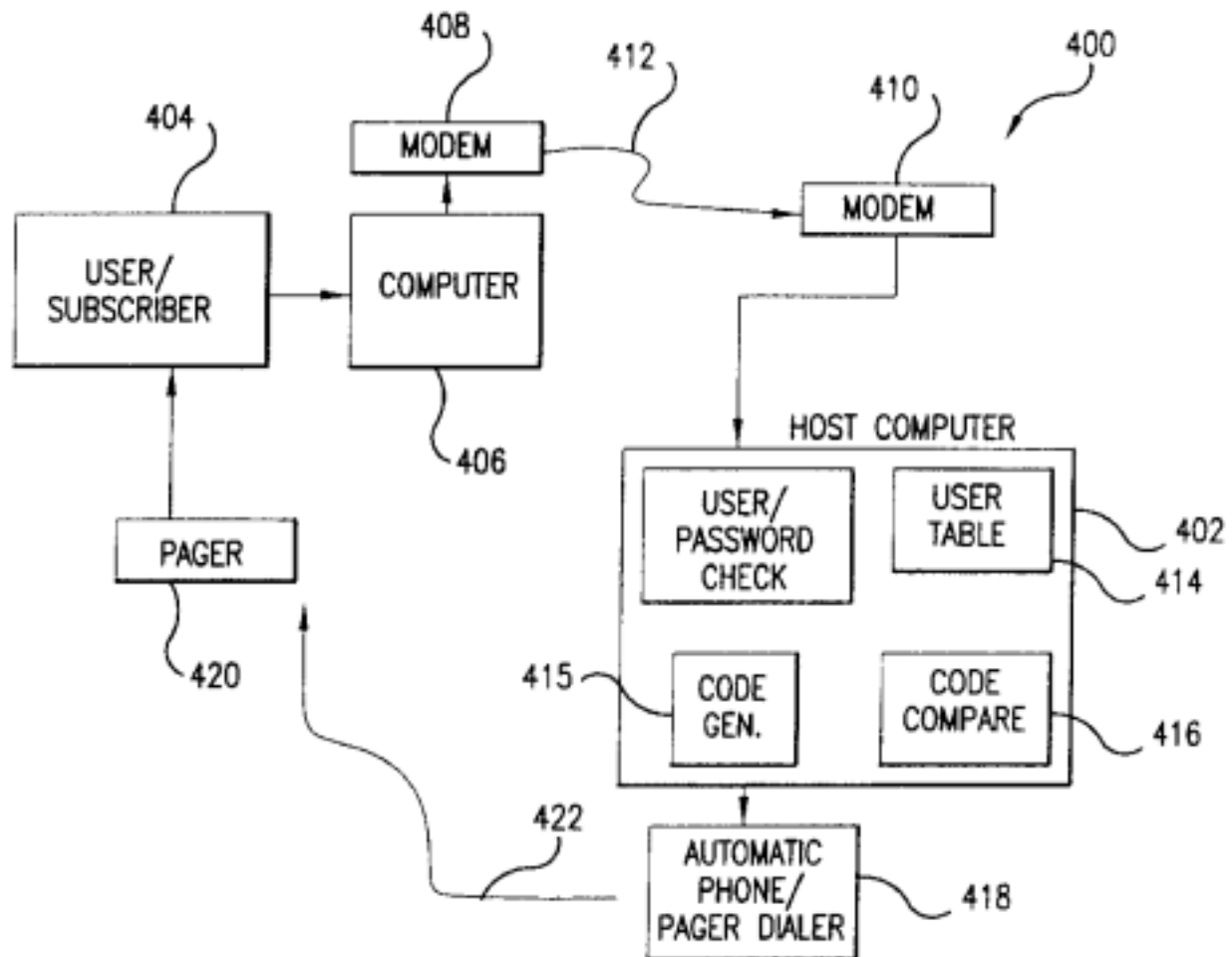


FIG. 6

72. Therefore, it is my opinion that a POSITA would have understood that *Veneklas* teaches *user authentication system* (e.g., adapted to grant an authorized individual access).

[5.1] a computer processor;

73. It is my opinion that a POSITA would have understood that *Veneklas* teaches this limitation; any alleged differences would have been obvious. Specifically, *Veneklas* discloses that analyzing means 12 may comprise a

microprocessor and/or similar type of computer.” EX1005, 5:35-37, Fig. 1.

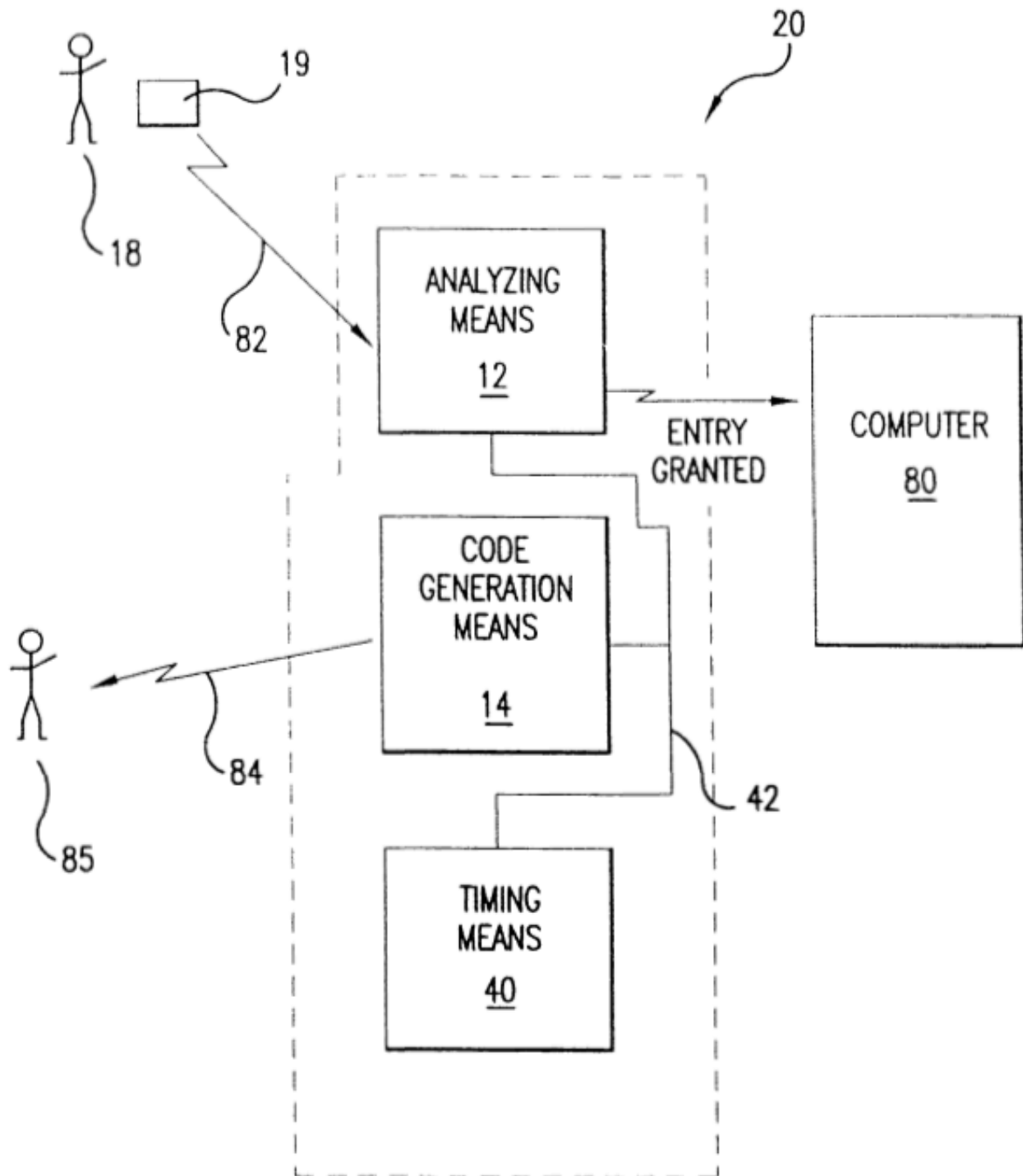
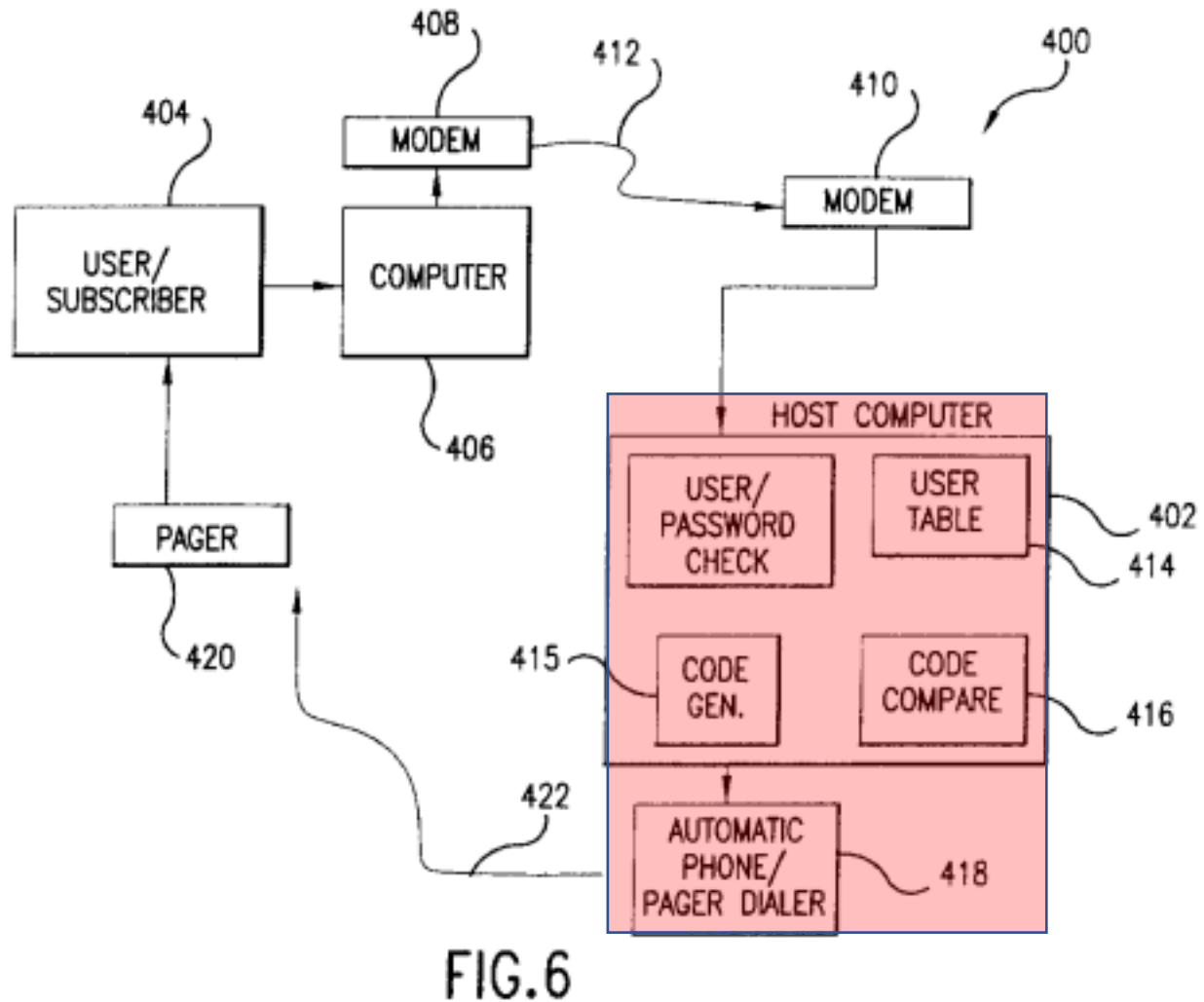


FIG.1

74. *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.

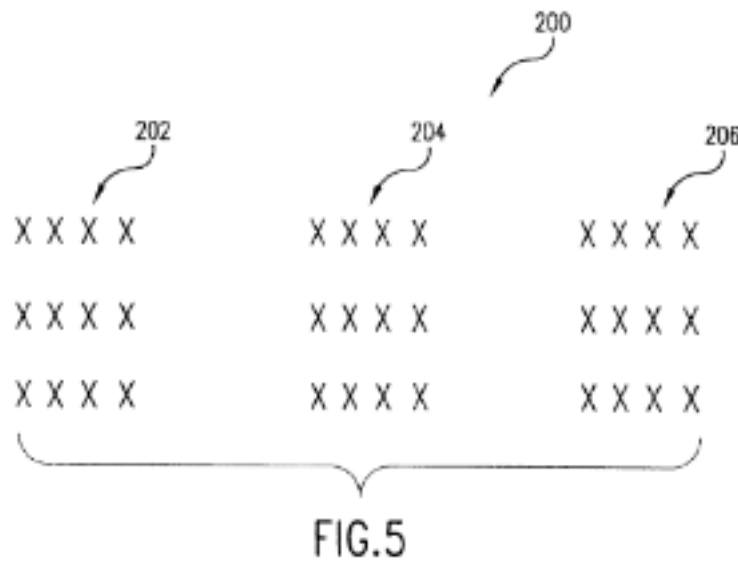


75. In is my opinion that a POSITA would have understood that a computer capable of all of these actions, including checking codes against a database and generating random numbers would necessarily contain a computer processor.

76. Therefore, it is my opinion that a POSITA would have understood that *Veneklase* teaches a computer processor (e.g., microprocessor).

[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;

77. It is my opinion that a POSITA would have understood that *Veneklas* teaches this limitation; any alleged differences would have been obvious. *Veneklas* 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).



78. Furthermore, Veneklasе 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.

79. *Veneklasе* additionally teaches the second half of this limitation (*i.e., 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.

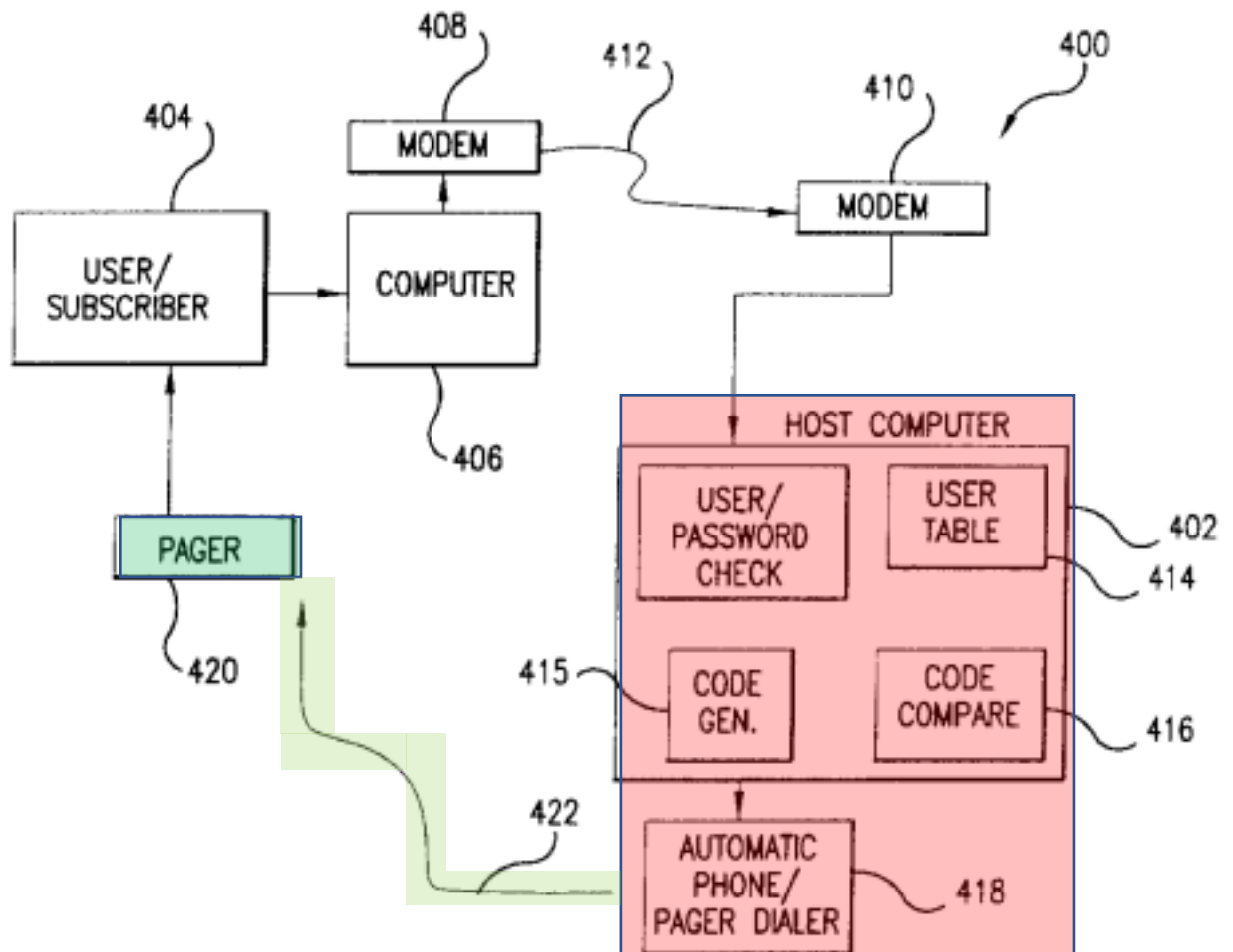


FIG. 6

80. 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. 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, 5:34-40; *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.

81. To the extent it is argued that the pager network disclosed in *Veneklase* does not satisfy the cell phone network requirement, a POSITA would have found it obvious to implement the authentication system of *Veneklase* using a cell phone network. 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. 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. A POSITA at the time would have understood that cellular phones were becoming more readily available, less expensive, and through the availability of Short Message Service (SMS), also known as “texting,” a cellular phone network could perform all the functions previously provided by a paging network using a multifunction device. The concept of SMS was first proposed in 1984 for GSM, so by 2000 it would have been well known to a POSITA working with mobile wireless networks. *See, e.g.*, EX1016, 1. Pagers were also limited function devices, with little processing power and generally no programmability. Cell phones, in contrast, had richer user interfaces, more processing capacity, and often programmability to allow extension to their functionality. 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. While the specific radio interfaces may differ between pagers and cellular SMS messaging, both present standardized interfaces to the external systems. With the widespread use of the Internet, it is common to provide an Internet Protocol (IP) gateway or a specific Applications Program Interface (API) to allow messages to be passed to either paging or SMS systems.

82. Therefore, it is my opinion that a POSITA would have understood that *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).

[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;

83. It is my opinion that a POSITA would have understood that *Veneklase* in combination with *Jonsson* teaches this limitation; any alleged differences would have been obvious. *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.

84. Thus, *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 in Figure 6. EX1005, Fig. 6.

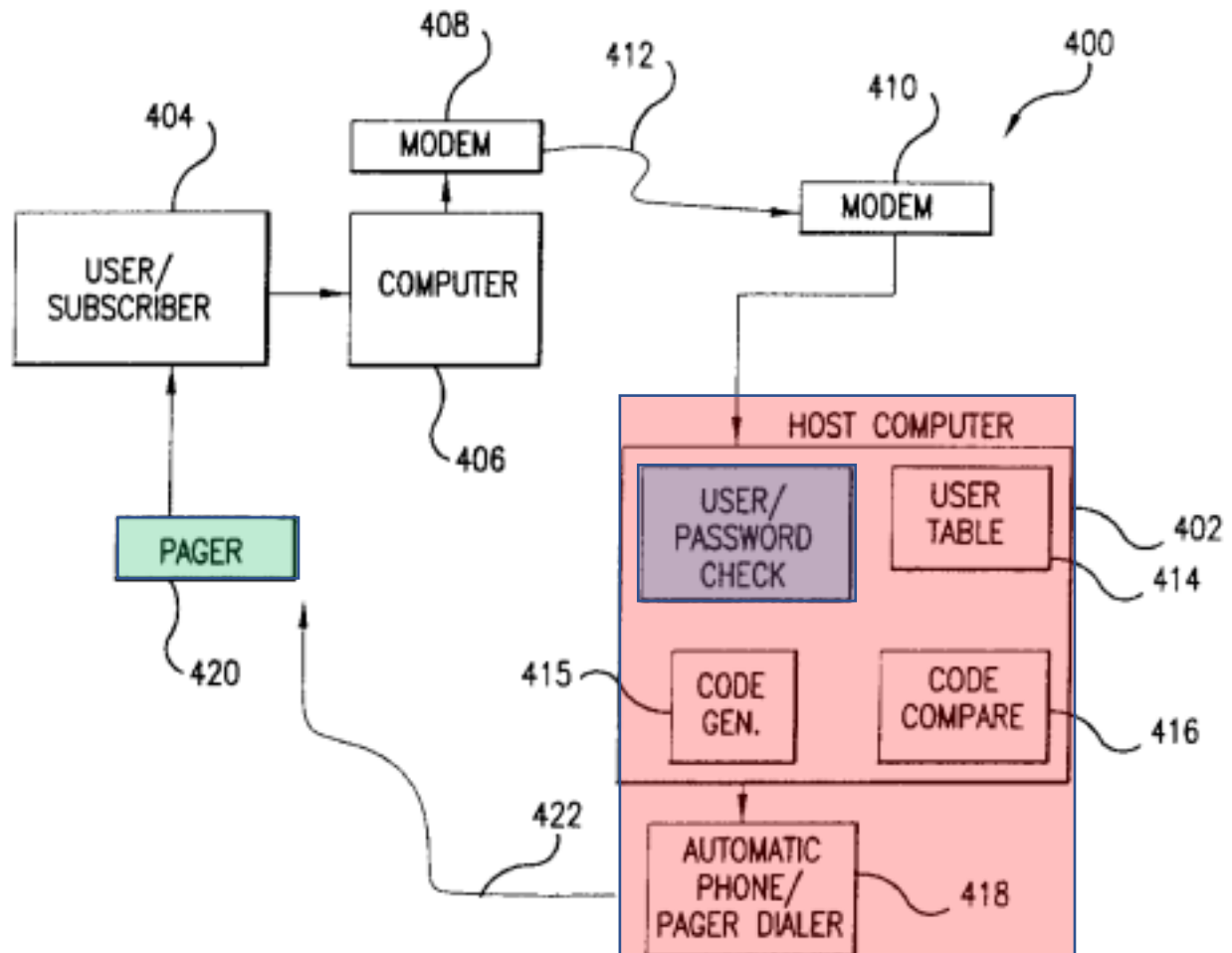


FIG.6

85. 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.

86. 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, a POSITA would have found it 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).

87. 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. 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”).

88. *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. 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). Furthermore, it would have been understood by a POSITA to be new since it is unique to each transaction and thus not a reused response code.

89. When combined, *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).

90. Therefore, it is my opinion that a POSITA would have understood that *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).

Motivations to Combine *Veneklase* and *Jonsson*

91. 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. *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. *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. 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.

92. 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 Intern. Co. v. Teleflex Inc.*, 550 U.S. 398, 418-19 (2007). 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.

93. 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.* 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). 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.

94. 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.

95. 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.

96. 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 and setting that new

password to be the new password. 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

97. It is my opinion that a POSITA would have understood that *Veneklase* teaches this limitation; any alleged differences would have been obvious. *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.

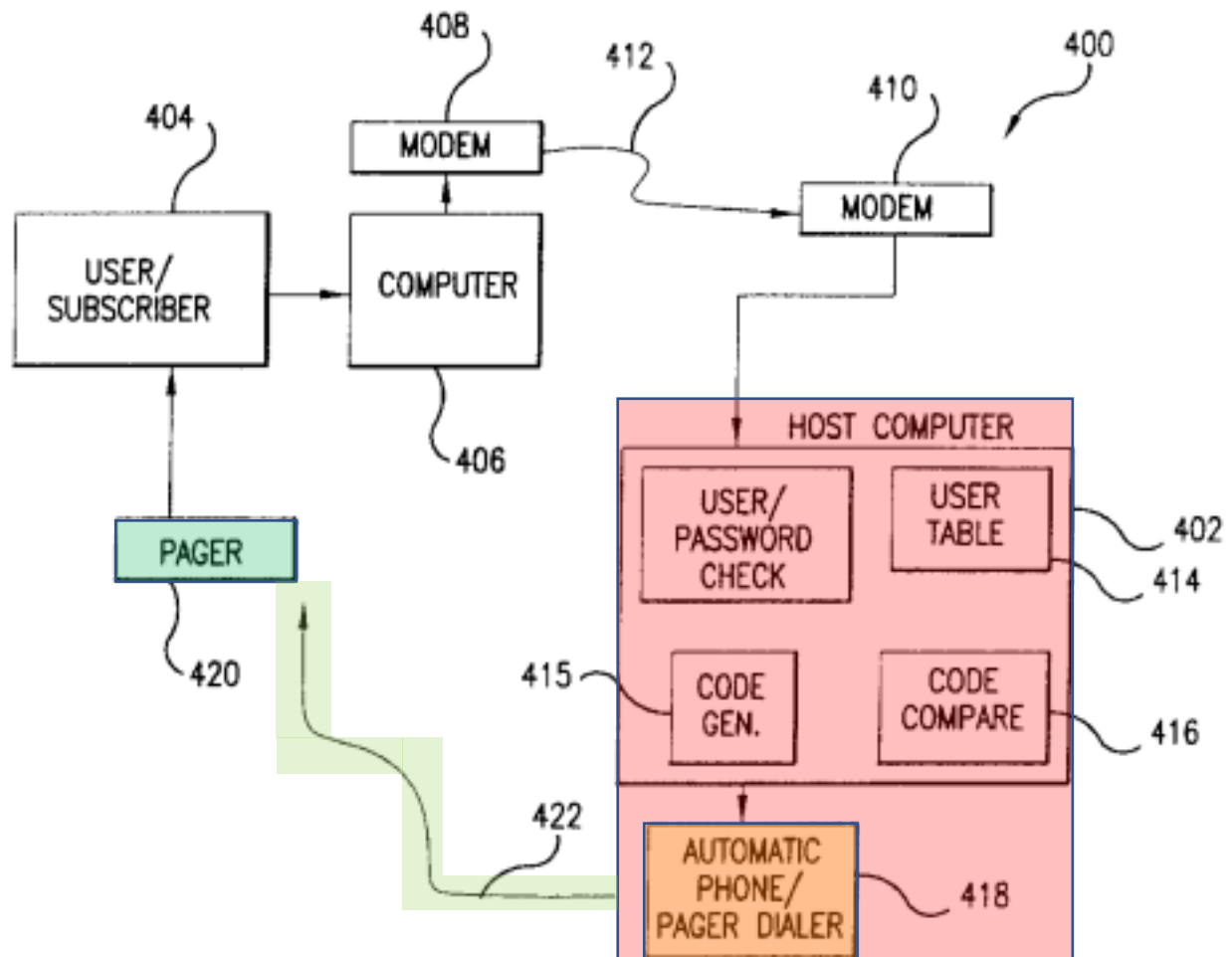


FIG. 6

98. 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. 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.

99. 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*. Furthermore, claim 1 also requires a personal communication device be in communication over a “cell phone network” and dependent claim 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, it is clear that the “cell phone network” claimed in the ’658 Patent also includes a pager network, as disclosed in *Veneklase*.

100. Therefore, it is my opinion that a POSITA would have understood that

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).

[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,

101. It is my opinion that a POSITA would have understood that *Veneklase*, alone or in combination with *Jonsson*, teaches this limitation; any alleged differences would have been obvious. *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.*

102. 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). A POSITA would have understood this to be the case because there is no other information that can be appropriately compared and this would be recognized by a POSITA as the standard technique used in various one-time password schemes.

103. *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).

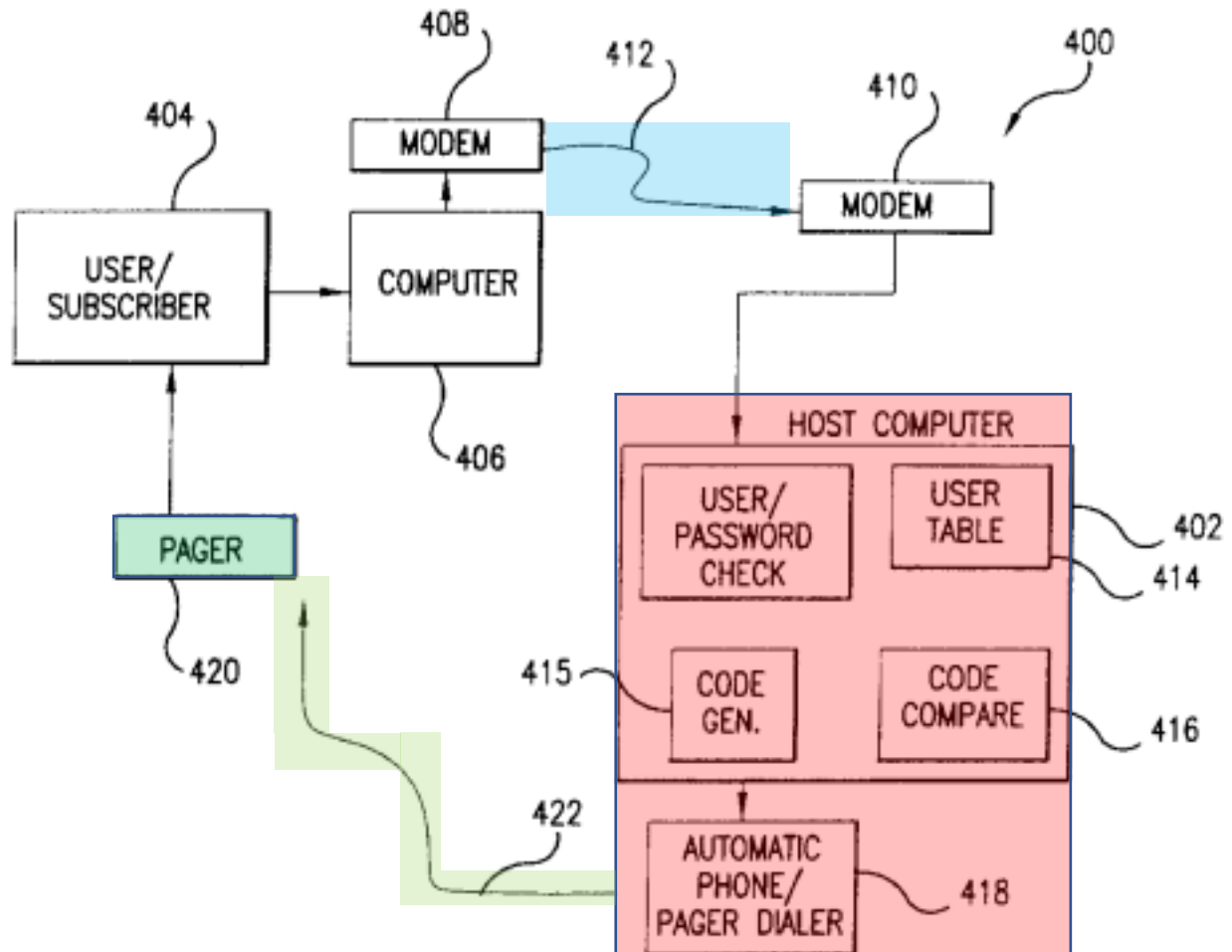


FIG. 6

104. 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”). 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.

105. Therefore, it is my opinion that a POSITA would have understood that *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).

[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.

106. It is my opinion that a POSITA would have understood that *Veneklase*, in combination with *Jonsson*, teaches this limitation; any alleged differences would have been obvious. *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.

107. 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.

108. *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*.

109. In the combination with *Jonsson* that I 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). 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).

110. *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.”).

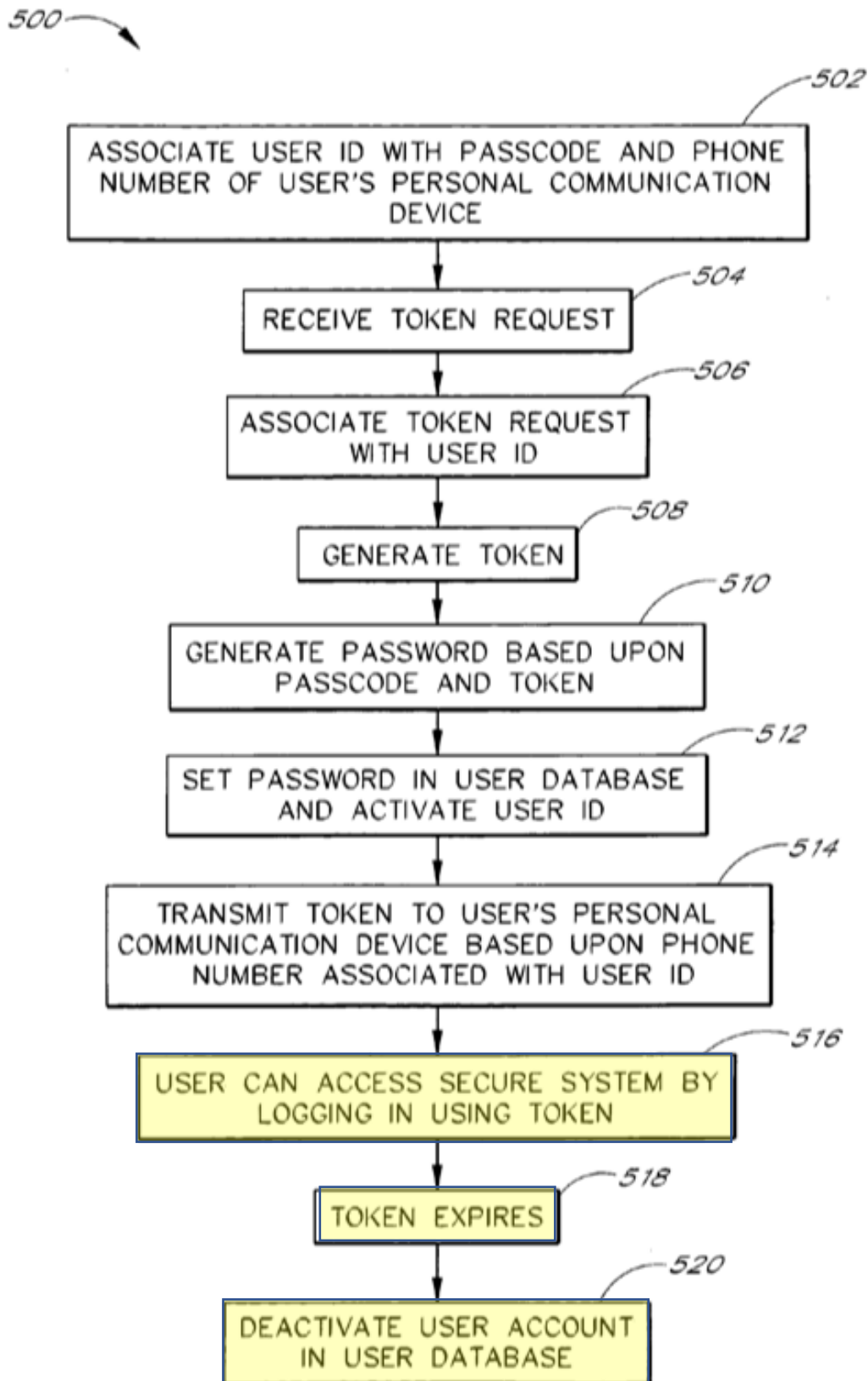


FIG. 5

111. Therefore, it is my opinion that a POSITA would have understood that *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).

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

i. Overview of Kew

112. *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.

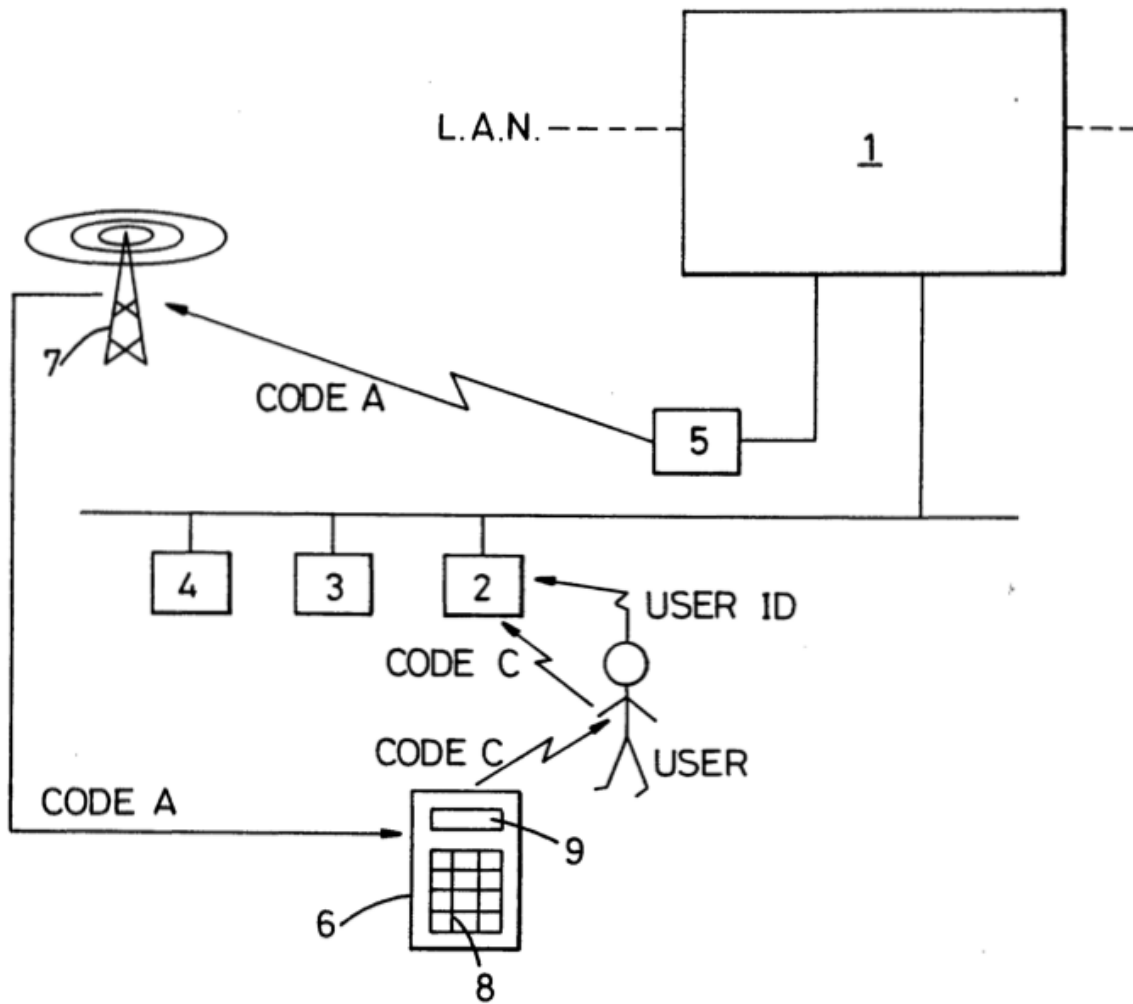
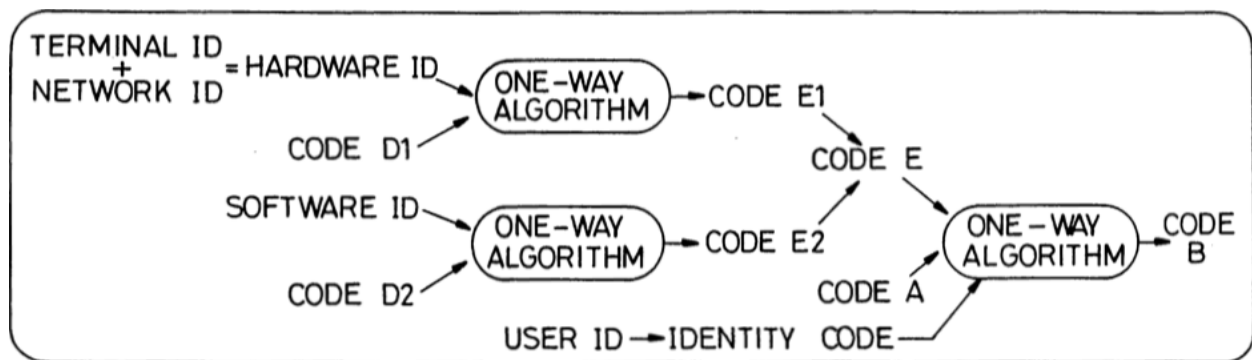


Fig. 1

113. 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.



114. “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.

ii. Overview of Sormunen

115. *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.

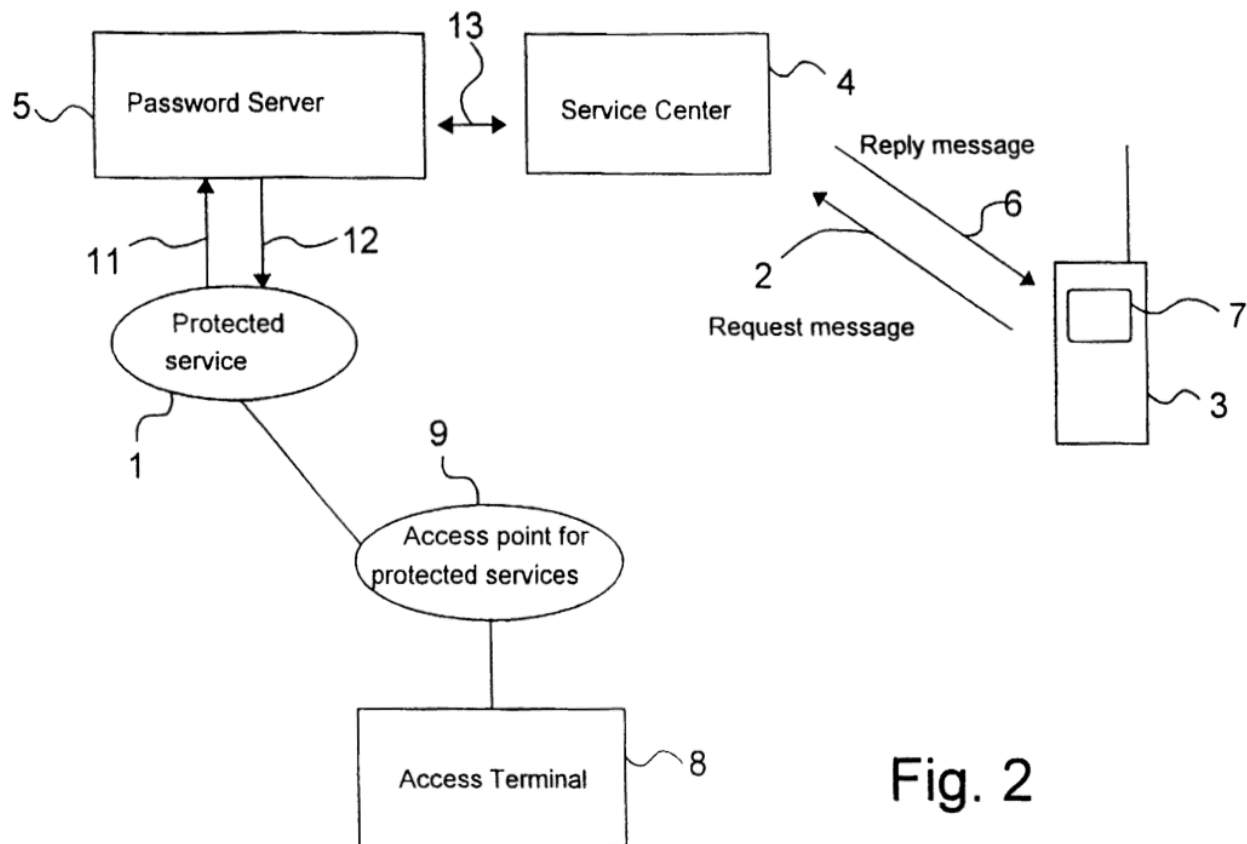


Fig. 2

116. *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.

117. *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.

iii. Analogous Art

118. *Kew* and *Sormunen* are analogous art. Both 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 (“relate[] 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 (“method of preventing unauthorised access to a host computer system”); EX1006, 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”).

119. In addition, each of these references is reasonably pertinent to at least one problem that would have concerned the inventor of the ’658 Patent. *Id.* The ’658 Patent purported to solve the problem in which 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, *Kew*’s system solves the same problem using a generated random code sent via radiofrequency transmission, “in a fashion similar to conventional paging systems.” *See, e.g.*, EX1005, 8:15-19. Similarly, *Sormunen*’s system seeks to solve that problem by sending authentication information to the user via a mobile network. *See, e.g.*, EX1006, 4:30-5:8.

iv. Claim 5

[5.0] A user authentication system comprising

120. I have been informed by counsel that, as a matter of law, the preamble may or may not limit the scope of the claims. To the extent the preamble is deemed limiting, it is my opinion that a POSITA would have understood that *Kew* teaches it; any alleged differences would have been obvious. *Kew* discloses “a method of

preventing unauthorized access to a host computer system.” EX1007, Abstract;
see also 1:3-15, Fig. 1.

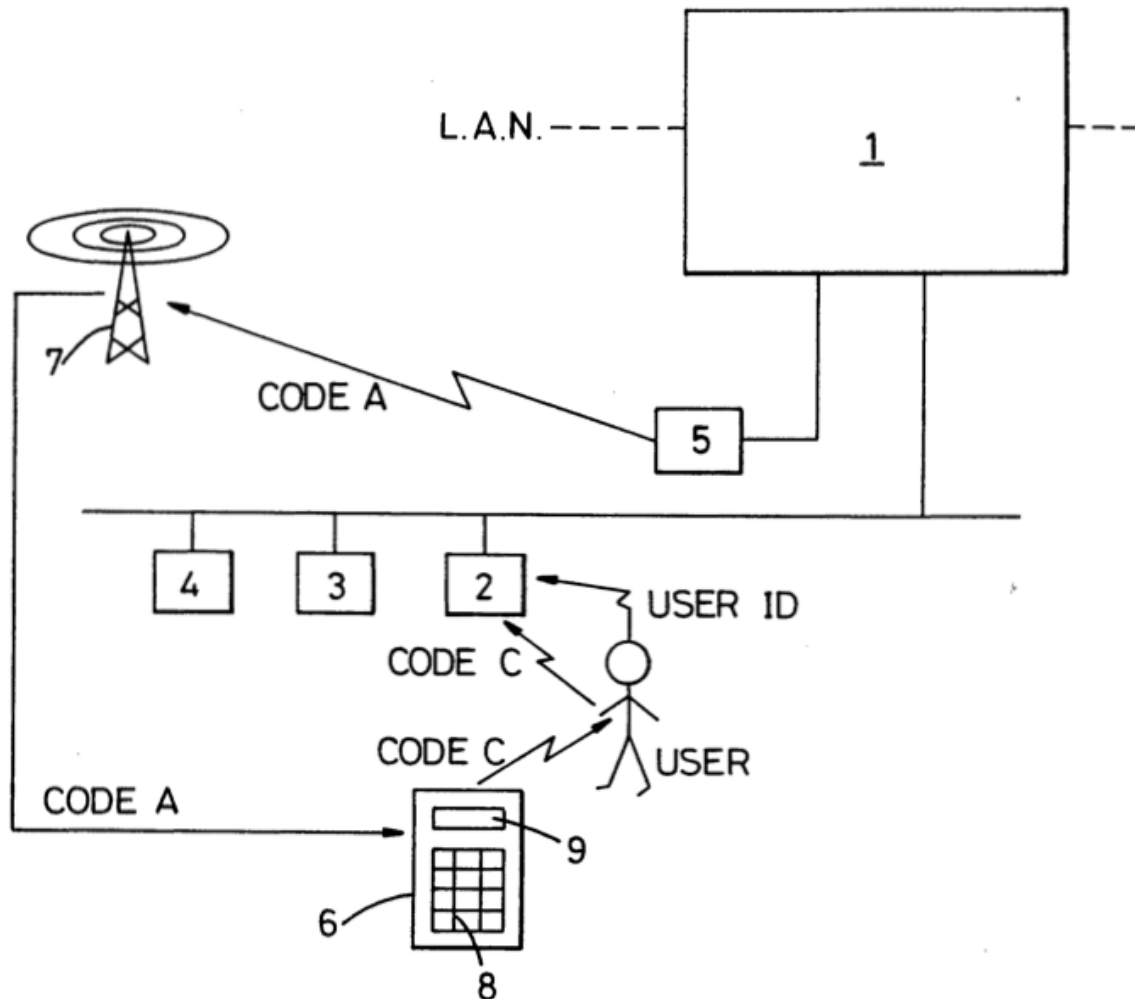


Fig. 1

121. Therefore, it is my opinion that a POSITA would have understood that
Kew teaches *user authentication system* (e.g., authorization system).

[5.1] a computer processor;

122. It is my opinion that a POSITA would have understood that *Kew* teaches this limitation; any alleged differences would have been obvious. 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.

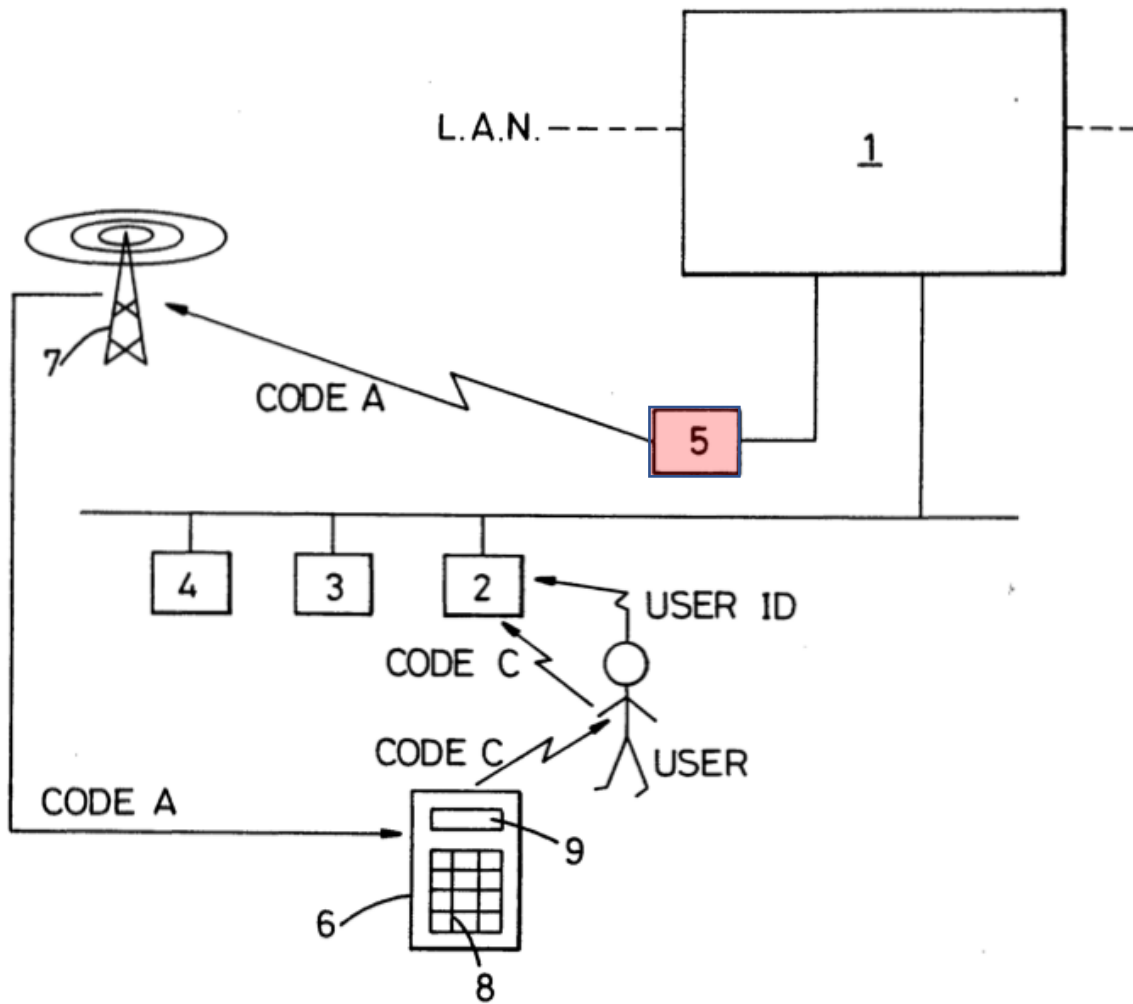


Fig. 1

123. 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. It would have been apparent to a POSITA that the terminal 2 and the security server 5 must perform certain algorithms to engage in the authentication protocol described and to interact with the user. A POSITA would have understood that these

operations would have been performed by using an appropriately programmed central processing unit contained within these devices.

124. Therefore, it is my opinion that a POSITA would have understood that *Kew* teaches *a computer processor* (e.g., central processing unit).

[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;

125. It is my opinion that a POSITA would have understood that *Kew*, alone or in combination with *Sormunen*, teaches this limitation; any alleged differences would have been obvious. *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.

126. *Kew* additionally teaches the second half of this limitation (*i.e., 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. 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, 5:34-40; *see also* Abstract, 1:10-11, 2:6-8, 2:28-31, 3:1-3, 4:13-17, 9:45-54. 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

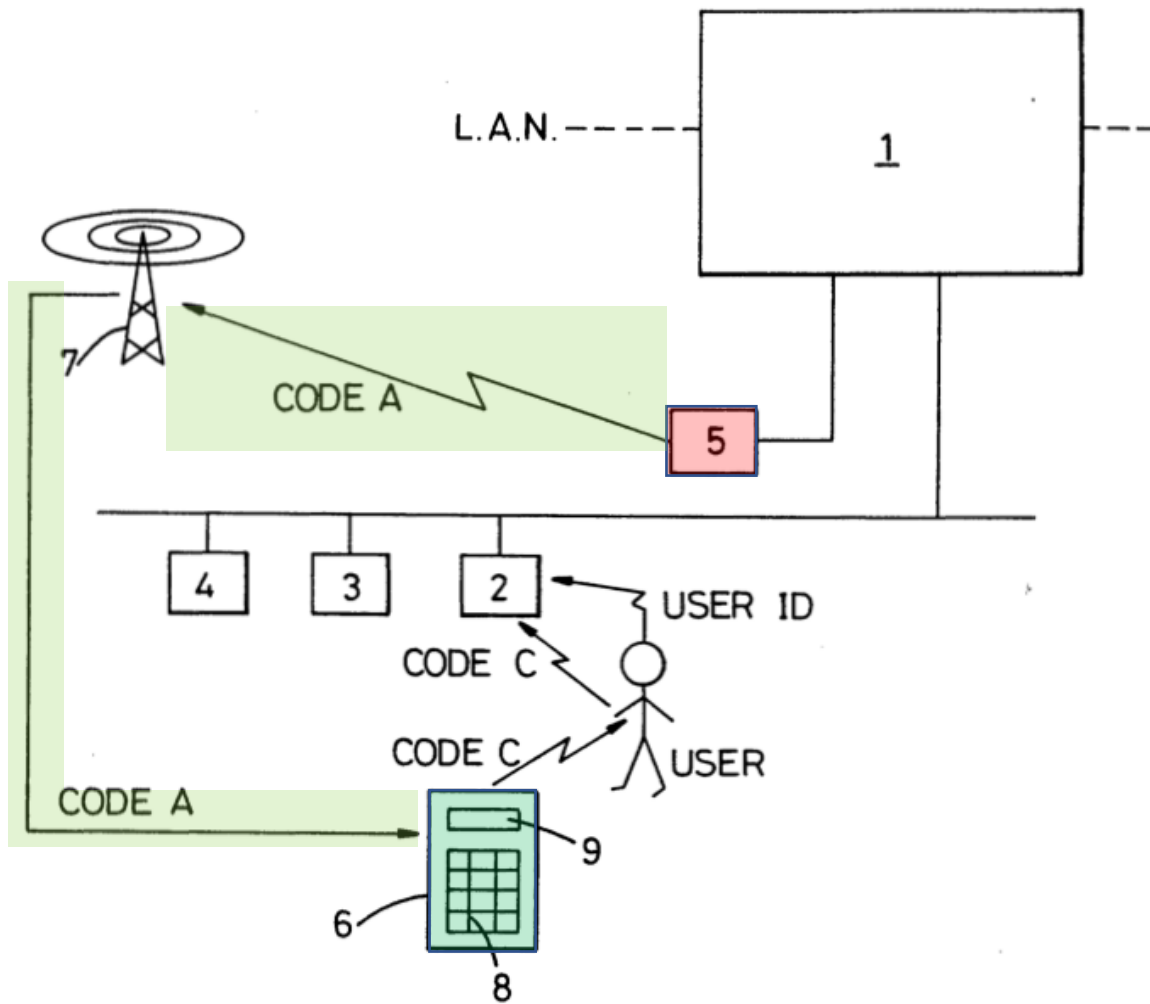


Fig. 1

127. 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. 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. For the reasons I discussed above regarding claim element [5.2] of Ground 1, a POSITA would have recognized that a cellular network's SMS functionality could equivalently be used. 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. 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. 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.

128. Therefore, it is my opinion that a POSITA would have understood that *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).

129. To the extent it is argued *Kew* does not teach or render obvious the use of a cell phone network, a POSITA would have understood that *Sormunen* discloses a *personal communication device* (e.g., paging device 3) *configured to communicate over a cell phone network* (e.g., cellular network). 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.

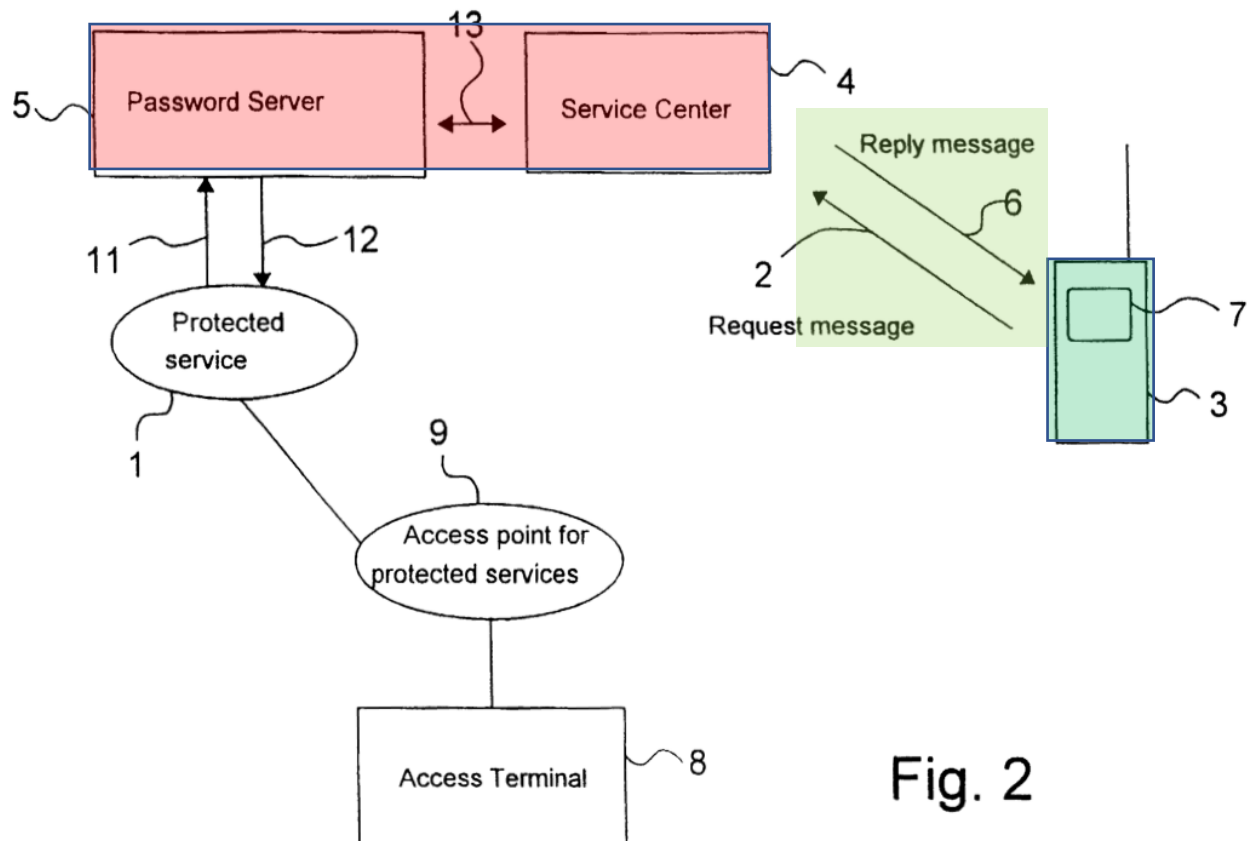


Fig. 2

130. *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*

131. 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. *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. 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.

132. 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.

133. 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 *Kewe* because it would have been used in the same way, i.e., to allow

communication between a mobile device unit and a central server. 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.

134. 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*.

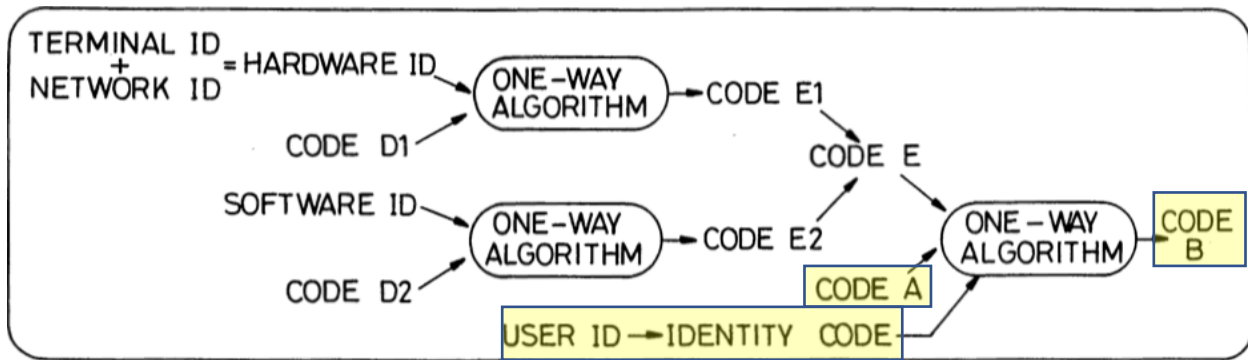
135. Therefore, a POSITA would have been motivated to modify, and would have had a reasonable expectation of success in modifying, *Kew*'s authentication system to include *Sormunen*'s teachings related to the use of a cellular network. Thus, *Kew*, in combination with *Sormunen*, teaches this limitation.

[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;

136. It is my opinion that a POSITA would have understood that *Kew* teaches this limitation; any alleged differences would have been obvious. *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.

137. *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.



138. 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.

139. *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. This kind of new password creation was well known in the prior art. For instance, in RFC2289, the initial step takes a user's secret pass-phrase (which is like an arbitrary length password) and concatenates it with a random seed that is transmitted from the server in the clear. *See, e.g.*, EX1011. This pass-phrase plus seed is run through a secure (non-linear and non-invertible) hash function creating a 64-bit value. Each time the computation step is run it generates a one-time password by applying the secure hash function to the output of the initial step. *Id.* The server and the user know the secret pass-phase and the seed, the hashing function, and the number of times to apply the hash function. *Id.* Successively re-running the hash function can generate a sequence of passwords that are each only used once. *Id.*

140. *Therefore*, it is my opinion that a POSITA would have understood that *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).

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

141. It is my opinion that a POSITA would have understood that *Kew* teaches this limitation; any alleged differences would have been obvious. 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.

142. 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. This is very similar to what is disclosed in *Kew*.

Furthermore, claim 1 also requires a personal communication device be in communication over a “cell phone network” and dependent claim 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, it is clear that the “cell phone network” claimed in the ’658 Patent also includes the pager network, as disclosed in *Kew*.

143. Therefore, it is my opinion that a POSITA would have understood that *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).

[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,

144. It is my opinion that a POSITA would have understood that *Kew* teaches this limitation; any alleged differences would have been obvious. *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.

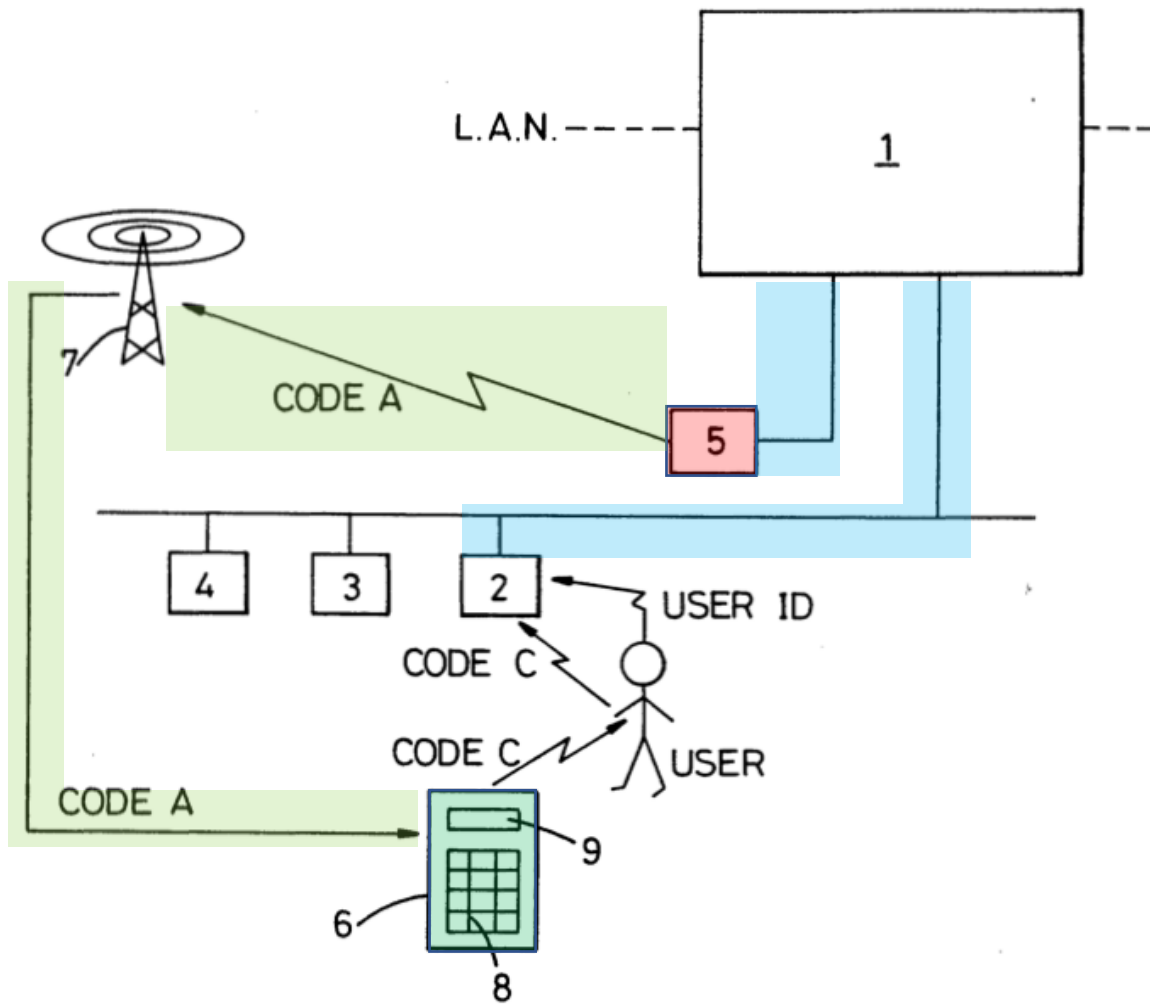


Fig. 1

145. A POSITA would have understood that this connection, which is clearly 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. 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. Further, this makes sense because a POSITA would recognize that whenever two or more separate communications paths are used for a transaction, there is inherently more security than for a single path since an attacker would need to access additional communications paths to complete the transaction instead of just one.

146. Therefore, it is my opinion that a POSITA would have understood that *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).

[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.

147. It is my opinion that a POSITA would have understood that *Kew*

teaches this limitation; any alleged differences would have been obvious. *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, it produced by encryption of the random code, Code A” 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.

148. 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. As I discuss in the background section above, authentication security services must be built on top of identification security services – a POSITA would recognize that it is first necessary to identify an entity and establish that they are a valid user of a system before authentication of

that entity can occur. Otherwise, there can be no basis to validate the correctness of any authentication.

149. 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.

150. *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, preferably a liquid crystal display, 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. 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. A POSITA would have understood that this is just an example of the well-known concept of time-bound access, which I discuss in the technology background section above.

151. *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.").

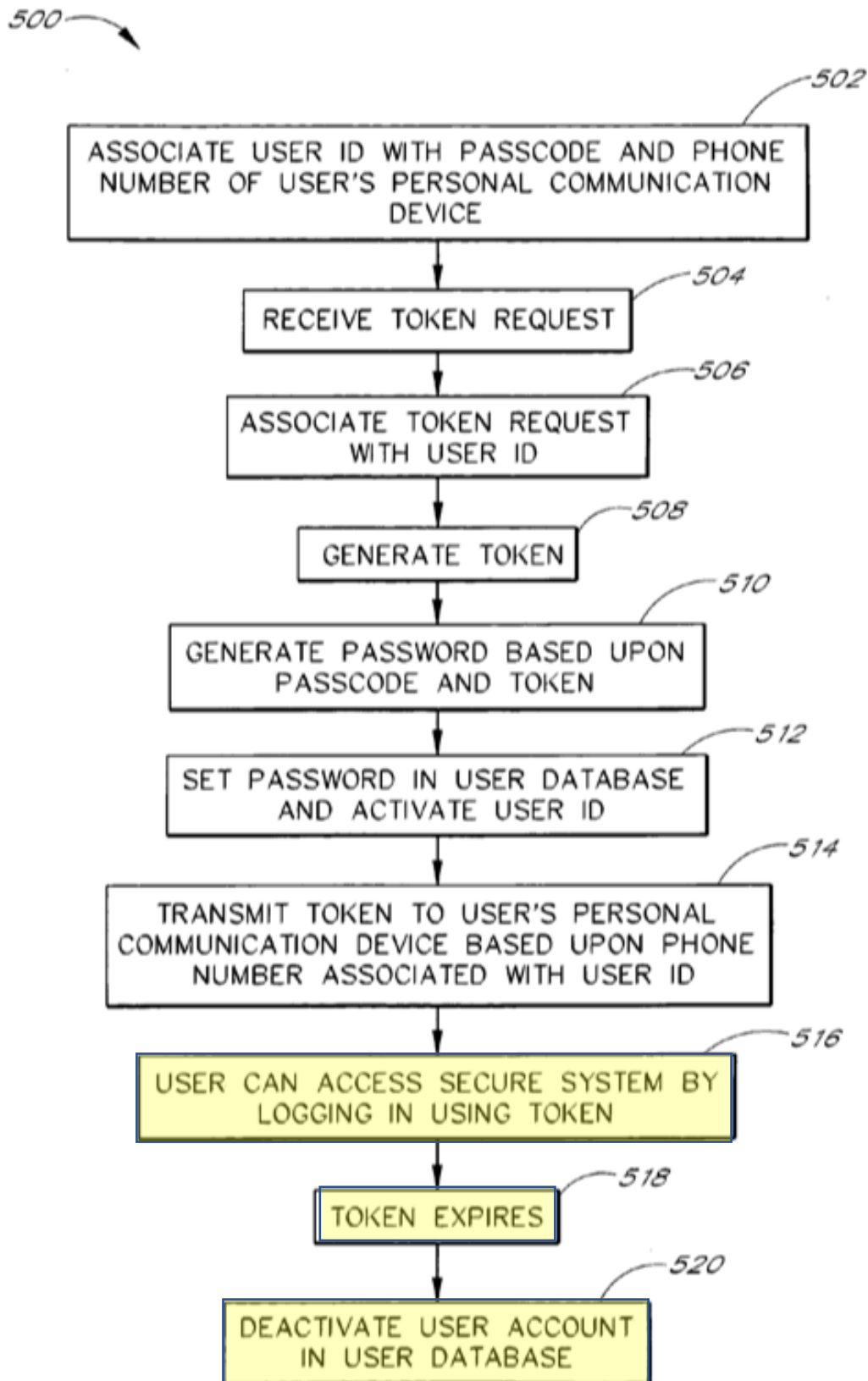


FIG. 5

JPMORGAN EXHIBIT 1003

152. Therefore, it is my opinion that a POSITA would have understood that *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).*

v. **Claim 6**

[6.0] The system of claim 5,

153. It is my opinion that a POSITA would have understood that *Kew* in view of *Sormunen* renders obvious claim 5. See Sec. VII.B.iv, above.

[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.

154. It is my opinion that a POSITA would have understood that *Kew* teaches this limitation; any alleged differences would have been obvious. *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 from the user, “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. A POSITA would recognize that both in *Kew* and in the ‘658 Patent the token request and generation of a password are the standard mechanisms used in one-time password schemes that were commonly used in the prior art.

155. Therefore, it is my opinion that a POSITA would have understood that *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).

vi. **Claim 1**

156. Most limitations of claim 1 are substantively similar to claim 5. Therefore, It is my opinion that a POSITA would have understood that 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*.

<i>Claim 1</i>		<i>Cross-References</i>
[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]
[1.2]	<i>receiving a request from the user for a token via the personal communication device, over the second network;</i>	See <i>infra</i>
[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;

157. It is my opinion that a POSITA would have understood that *Kew*, in combination with *Sormunen*, teaches this limitation; any alleged differences would have been obvious. 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.

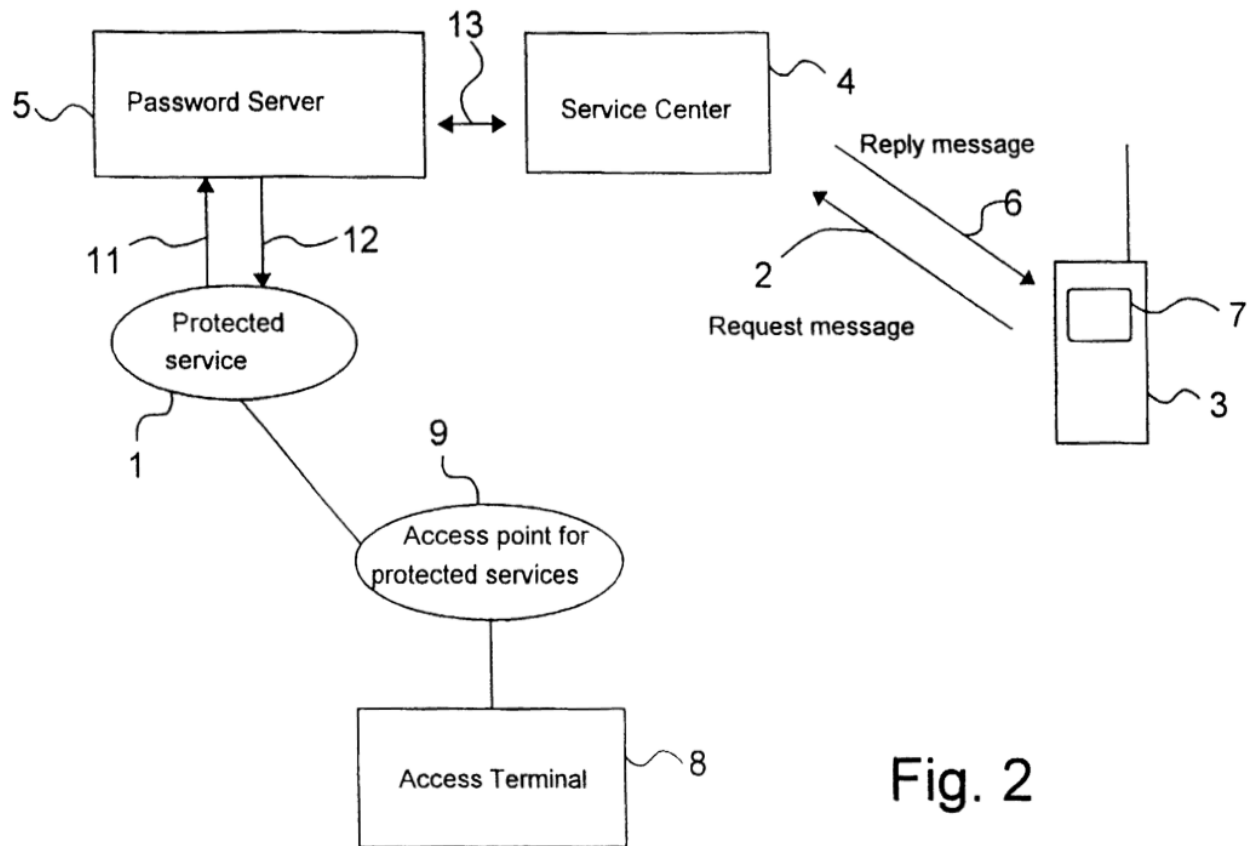


Fig. 2

158. *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)).

159. 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 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.

160. Therefore, it is my opinion that a POSITA would have understood that *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).

vii. **Claim 3**

[3.0] The method of claim 1,

161. *Kew* in view of *Sormunen* renders obvious claim 1. See Sec. VII.B.vi.

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

162. It is my opinion that a POSITA would have understood that *Kew*, in combination with *Sormunen*, teaches this limitation; any alleged differences would have been obvious. *Sormunen* discloses that *the personal communication device* is a “paging terminal 3, such as a mobile station.” EX1008, 5:35-38, Fig. 2.

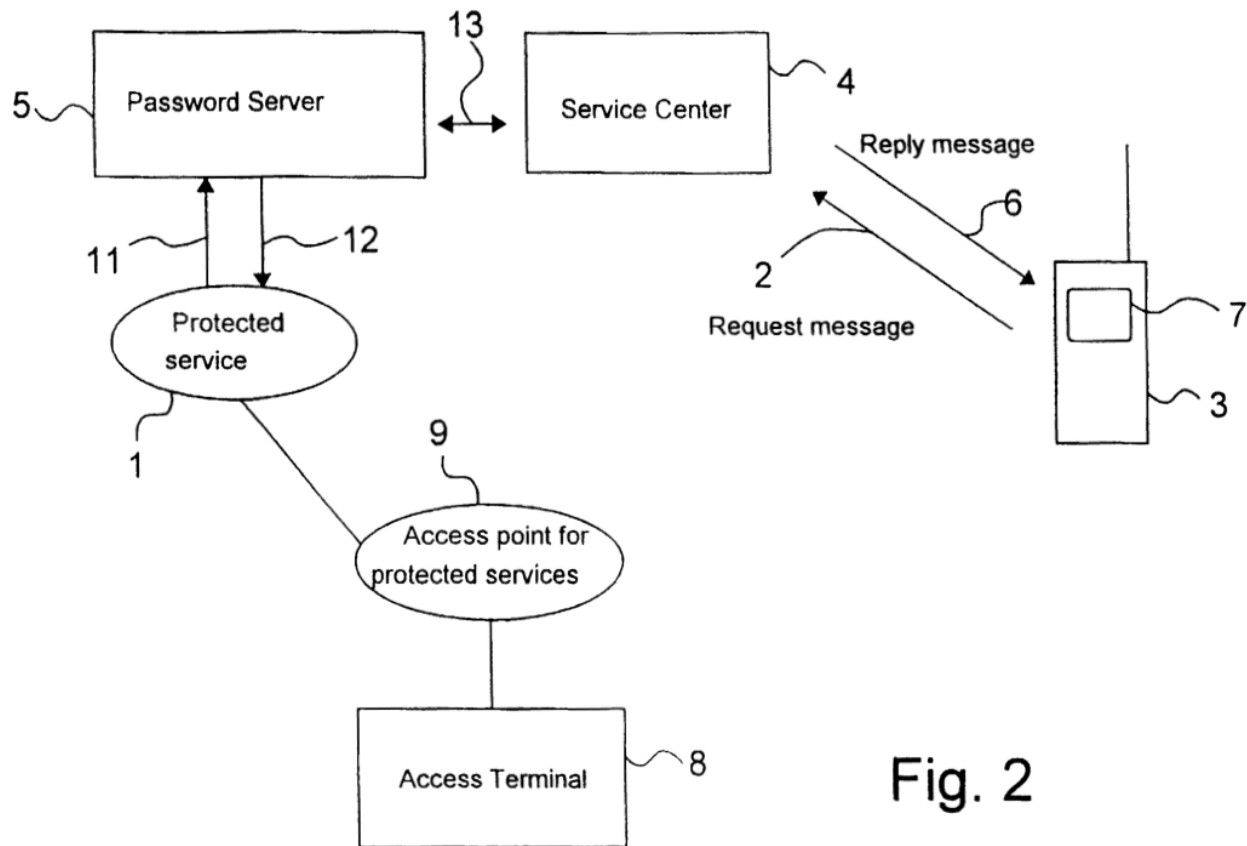


Fig. 2

163. *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. Thus, a POSITA would understand *Sormunen* to disclose that the mobile station can be a mobile phone.

164. Therefore, it is my opinion that a POSITA would have understood that

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).

viii. Claim 4

[4.0] The method of claim 1,

165. *Kew* in view of *Sormunen* renders obvious claim 1. *See* Sec. VII.B.vi.

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

166. It is my opinion that a POSITA would have understood that *Kew*, alone or in combination with *Sormunen*, teaches this limitation; any alleged differences would have been obvious. 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.

167. Therefore, it is my opinion that a POSITA would have understood that *Kew*, alone or in combination with *Sormunen*, teaches *wherein the personal communication device is a pager* (e.g., receiver that receives pages).

VIII. CONCLUSION

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

Date: January 6, 2023

By: 
Bruce McNair