

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

EXPERIAN INFORMATION SOLUTIONS, INC.,

Petitioner,

v.

DYNAPASS IP HOLDINGS LLC,

Patent Owner.

U.S. Patent No. 6,993,658

Inter Partes Review No.: IPR2023-01406

**DECLARATION OF STEPHEN PERKINS, PH.D.
IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 6,993,658**

TABLE OF CONTENTS

I.	Introduction.....	1
II.	List of Documents I Considered in Forming My Opinions	1
III.	My Background and Qualifications	3
IV.	Relevant Legal Standards.....	11
	A. Obviousness Generally.....	12
	1. The POSA Requirement	12
	2. The Obviousness Inquiry	13
	B. Analogous Art	16
	C. Objective Indicia of Nonobviousness	17
V.	The Level of Ordinary Skill in the Art	18
VI.	The '658 Patent	19
	A. Summary	19
	B. Prosecution History	25
	C. Priority Date of Claims	31
VII.	State of the Art.....	32
	A. Two-Factor Authentication	32
	B. The Use of Different Communication Networks	34
	C. The Use of Cell Phones and Pagers for Two-Factor Authentication.....	35
	D. Concatenation for Passwords	40
	E. Databases.....	47
VIII.	Claim Construction.....	50

A.	Preambles	50
B.	Order of Steps.....	51
C.	Passcode, Token, and Password	53
IX.	Claims 1-7 of the '658 Patent are Obvious Over the Sormunen in View of Perlman	54
A.	The Sormunen Reference	55
B.	The Perlman Reference	60
C.	Motivation to Combine the Teachings of Sormunen and Perlman	63
D.	Detailed Application of Sormunen and Perlman.....	67
1.	Claim 1	68
2.	Claim 2	81
3.	Claim 3	82
4.	Claim 4	83
5.	Claim 5	84
6.	Claim 6	92
7.	Claim 7	94
X.	Summary of My Opinions	95
XI.	Declaration.....	96

I, Stephen Perkins, declare as follows:

I. Introduction

1. I am over the age of eighteen (18) and otherwise competent to make this declaration.

2. I understand that Experian Information Solutions, Inc. (“Experian” or “Petitioner”) is submitting a petition for inter *partes* review of claims 1-7 of U.S. Patent No. 6,993,658 (“the ’658 Patent”) (Ex-1001). I have been retained by Experian as a technical expert to provide my independent opinions on certain issues relating to the petition.

3. I am being compensated at my rate of \$450 per hour for the time I spend on this matter. No part of my compensation depends on the content of this Declaration or the outcome of this proceeding, and I have no other interest in this proceeding.

4. I understand that the ’658 Patent was issued to April System Design AB. I understand that the ’658 Patent is now purportedly owned by Dynapass IP Holdings LLC (“Patent Owner”).

5. To the best of my knowledge, I have no financial interest in Experian or Patent Owner.

II. List of Documents I Considered in Forming My Opinions

6. In formulating my opinions, I have considered and relied on statements in the documents identified below. These documents include patents, published patent

applications, published textbooks, and other relevant documents. I consider each of the references below as a reliable authority for the statements on which I rely. I have considered these documents in light of the general knowledge of a person of skill in the art (“POSA”) as of March 6, 2000.

Exhibit #	Description
1001	U.S. Patent No. 6,993,658
1002	Certified File History for U.S. Patent No. 6,993,658
1004	PCT Publication No. WO 97/31306 (“Sormunen”)
1005	U.S. Patent No. 6,173,400 (“Perlman”)
1006	U.S. Patent No. 6,731,731 (“Ueshima”)
1007	U.S. Patent No. 5,881,226 (“Veneklase”)
1008	Japanese Patent Publication No. P2000-10927 (“Katou”)
1009	European Patent Publication No. EP1107089 (“Williamson”)
1010	U.S. Patent No. 5,787,169 (“Eldridge”)
1011	Hopcroft & Ullman, Introduction to Automata Theory, Languages, and Computation (1979) (ISBN: 0-201-02988-X)
1012	Carlo Ghezzi & Mehdi Jazayeri, Programming Language Concepts (1982) (ISBN 0-471-82173-X)
1013	Robert Sedgewick, Algorithms (1983) (ISBN 0-201-06672-6)
1014	Brian Kernighan & Dennis Ritchie, The C Programming Language (2d ed. 1988) (ISBN 0-13-110370-9)
1015	U.S. Patent No. 6,496,477 (Stephen J. Perkins, et al.)
1016	M. Wahl, “A Summary of the X.500(96) User Schema for use with LDAPv3,” RFC2256, Dec. 1997

III. My Background and Qualifications

7. A list of my publications and patents is contained in my curriculum vitae, attached hereto as Appendix A. I have not testified as an expert at trial, hearing, or deposition in the last ten years.

8. I received my Bachelors of Science and Masters of Science in Computer Science from Texas A&M University in College Station in 1989 and 1991 respectively. I completed a Ph.D. in Computer Science from Michigan State University in 1997.

9. I have over 35 years of industry experience in the areas of digital signal processing, wired and wireless networking, system architecture, system integration, distributed data storage, and software development. I highlight below some of my experience.

10. In the mid-1990's, dial-up modems were one of the primary means of connecting a computer system to other computer systems. Many users would dial into dedicated bulletin boards to read and post messages. There were also protocols available that would allow you to dial-in to a service provider and transmit and receive data that was not destined for a bulletin board, but for the Internet in general. These protocols allowed a computer system to send and receive IP datagrams over

a dial up phone connection. The Serial Line IP (SLIP¹) and Point-to-Point Protocol (PPP²) were the main methods in use.

11. I took it upon myself to port a version of the open-source Point-to-Point Protocol system (at that time maintained by Paul Mackerras) to a platform called NeXT (a platform created by Steve Jobs after he left Apple). I then maintained it. NeXT was a UNIX like operating system and the port of the PPP software required detailed knowledge of the operation of the kernel, network drivers, serial drivers, and TCP/IP networking. This work directly utilized dial-up modems and the public switched telephone network (PSTN).

12. I spent 13 years as a member of the technical staff at Texas Instruments (TI). One of my specific roles at TI was working with the Institute of Electrical and Electronics Engineers (IEEE) 802.14 subcommittee to develop a standard for cable modem systems. My area of specialty was the upstream communications area of the standard. As part of this work, our team at TI developed a working prototype of a complete cable modem system. This included both the portion that would eventually go into the home (i.e., the “cable modem”) and the portion that would reside at the service provider’s end (i.e. the “headend”). Also, as part of that work, we published

¹ A NONSTANDARD FOR TRANSMISSION OF IP DATAGRAMS OVER SERIAL LINES: SLIP; IETF RFC 1055; June 1998.

² The Point-to-Point Protocol (PPP); IETF RFC 1661; July 1994.

internal and external papers on the system. I am the lead author of a paper discussing the state of cable modems and the deployment of hybrid fiber-coax system as they existed in 1999.³

13. Another specific role that I had at TI was working with the team that was developing Digital Subscriber Line (DSL) technology. This was a competing networking technology that utilized copper phone wires for networking. In a DSL system, subscribers use DSL modems to connect to their service provider's network. The traffic from the DSL modem goes to a service provider network device called a Digital Subscriber Line Access Multiplexer (DSLAM). I am one of the authors of a TI publication titled "System Software of a DSP Based Digital Subscriber Line Access Multiplexer (DSLAM)"⁴ This paper discusses the software implementation of the DSLAM system on a Digital Signal Processor (DSP). A DSP is a specialized type of processor, as compared to the processors typically found in many PCs and servers.

14. Another role I had at TI was working with the HomePNA Alliance (known then as the Home Phoneline Networking Alliance or HPNA) to develop the

³ Stephen Perkins, Alan Gatherer: Two-way Broadband CATV-HFC Networks: State-of-the-Art and Future Trends. *Computer Networks* 31(4): 313-326 (1999).

⁴ Xiaolin Lu, Susan Yim, Steve Perkins: System Software of a DSP Based Digital Subscriber Line Access Multiplexer (DSLAM), Texas Instruments Communications Systems Engineering Branch, DSP R&D, February 17, 1999.

standard surrounding that medium of communication. This work led to communication protocols that worked over the copper phone lines or coax cable that was installed inside existing homes. It is my understanding that the HPNA protocol (along with its evolution over time) is still used with some AT&T and Cisco home gateways.

15. The above four roles dealt heavily with modems, communication protocols, and data communication over different mediums (PSTN dial-up networks, Hybrid Fiber-Coax broadband networks typically known as cable modem network, DSL broadband networks typically referred to as DSL or ADSL networks, and HPNA networks using pre-existing in home wiring).

16. I also have significant experience in wireless networks. My 1997 doctoral thesis, titled “Noise Tolerant Compression Protocols for Wireless Environments,”⁵ dealt specifically with data transmission over urban cellular radio environments (i.e., cell phone networks). It characterizes the issues that are faced when attempting to send data over wireless systems. It then presents solutions that improve the throughput of data sent over these networks and systems.

17. In 2018 I helped found a telecommunications startup. I was the technical lead for both the hardware team and the software development team. We

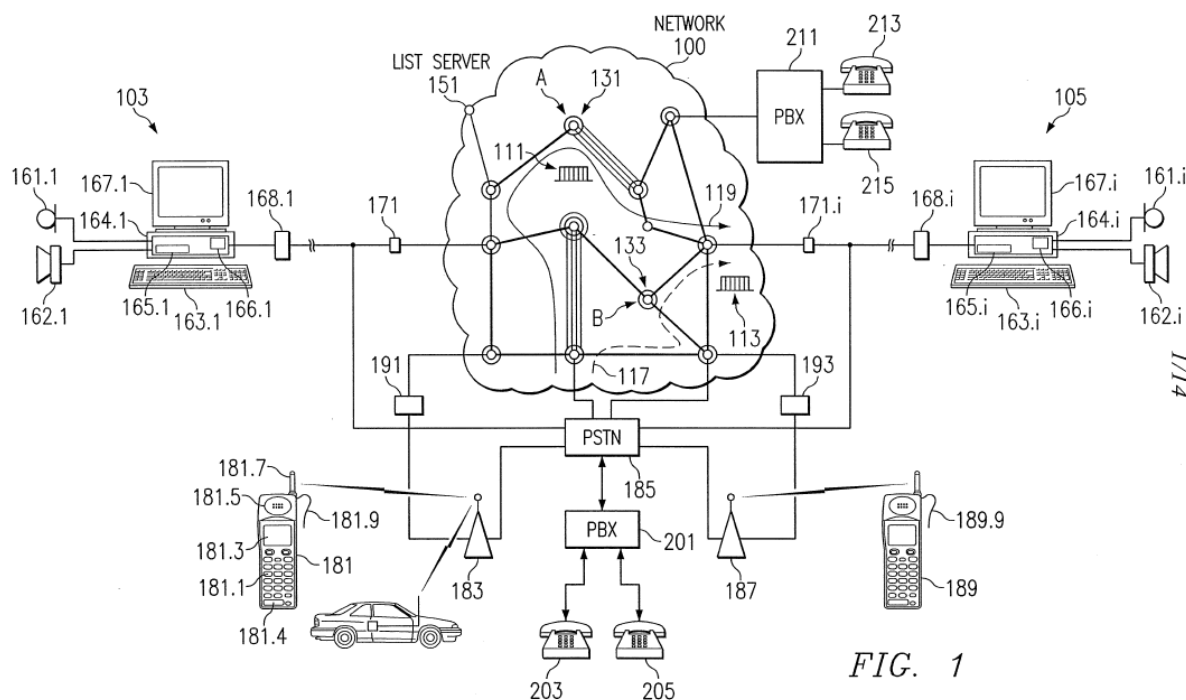
⁵ Publicly available from Michigan State University online at <https://d.lib.msu.edu/etd/26599>.

developed a postcard-sized communication module that bonded six 4G LTE cell phone network modems into a single network interface that maximized data throughput, network availability, and performance. Through these bonded modems, we were able to deliver data streams over multiple independent data channels. The data streams could be encrypted, prioritized, and securely transmitted across diverse paths over multiple cellular networks simultaneously. The system could be reconfigured to speak to different networks at will. Specifically, this work required detailed knowledge of the control and operation of Qualcomm 4G/LTE cell phone modems and their use on the respective cell phone networks (e.g., AT&T, Sprint, etc.). Since data could simultaneously travel across multiple providers' networks, and since the destination of the data was not necessary another cell phone, we were always sending data across multiple independent communications channels.

18. I am the lead inventor of patents related to network communication, including patents related to the utilization of path diversity (U.S. Patent Nos. 6,496,477, 6,930,983, 7,693,062, 8,396,058, 8,824,460, 7,961,758). These patents relate to communications channels that include personal computers (PC) or workstations as well as mobile terminals (cell phones and cell phone networks). As an example, see U.S. Patent No. 6,496,477 ("the '477 Patent") (Ex-1015). The 477 Patent issued from a patent application (No. 09/552,090) filed on April 19, 2000. However, it originally stems from a provisional patent application (No. 60/145,848)

filed on July 9, 1999.

19. The '477 Patent is entitled "Processes, Articles, and Packets for Network Path Diversity in Media over Packet Applications." The '477 Patent includes disclosure related to routing through multiple independent paths. Figure 1 of the '477 Patent shows a network incorporating workstations, mobile phones, a cellular network, and the public switched telephone network (PSTN). Ex-1015, 5:14-57, 6:18-7:50.



Ex-1015, Fig. 1.

20. In 1998 I helped found a company called NetMass Incorporated. This company is still in operation. NetMass is a Software as a Service (SAS) company that provides online computer backup. When we started, we provided all our services to end users who utilized dial-up modems to connect to the internet (most utilized the Point-to-Point protocol). Eventually, DSL and cable modems became available and made it into user's homes. We transitioned away from dial-up and over to broadband.

21. I have firsthand experience in the deployment and use of two-factor authentication systems. One of the things that we had to do with NetMass was provide very secure access to backend systems that spanned multiple data centers in multiple cities. To do this, we utilized commercial off the shelf (COTS) systems that provided virtual private networks (VPNs) and strong authentication. In 2004 NetMass purchased and then utilized a two-factor authentication system from a company called Authenex, Inc. ("Authenex"). Authenex was a competitor to RSA Security LLC and the Authenex system was a physical token-based system similar to the RSA SecureID system. I was the sole person who researched and compared the commercially available solutions, made the decision on which product to use, negotiated the purchase contract, bought, and then deployed to the systems inside NetMass. The use of the system required users to enter a password that consisted of the number displayed on the Authenex token appended to their private passcode.

Our employees used this system for years.

22. The wired and wireless network projects cited, my patent portfolio, my publications, and the companies I founded are intended to show that I have detailed knowledge of the systems, technologies, and the state of the art that was in play in 2000 at the time the '658 Patent was filed.

23. In 2012, I started teaching in the Department of Computer Science at the University of Texas Dallas. I started as an adjunct lecturer and came onboard full time as an assistant professor of instruction in 2016. Between 2016 and 2021 I was promoted to Associate Professor of Instruction and also became the Director of the Executive Master in Software Engineering (EMSE) program.

24. As an instructor, I taught foundational courses to students who were incoming freshman and I also taught upper-level elective courses to juniors and seniors who were getting ready to graduate. In 2018 I was nominated for the President's Teaching Excellence Award in Undergraduate Instruction. I received the best CS teaching faculty award in 2021.

25. As the Director of the EMSE program, I was directly involved with all operations of that program. Specifically, I was part of the group that evaluated incoming program candidates and I was part of the group that evaluated the curriculum. I also worked directly with each individual who was admitted to the program.

26. Between the two roles, I have a deep understanding of the level of skill that a student might have once they graduate with either a Bachelor or a Master of Science in Computer Science or in Software Engineering. Thus, I am familiar with the knowledge and capabilities of one of ordinary skill in the art. Unless otherwise stated, my testimony below refers to the knowledge of one of ordinary skill in the art as of March 6, 2000, the earliest possible effective filing date of the '658 Patent.

IV. Relevant Legal Standards

27. I am not a lawyer and am not offering any legal opinions. Although I am not a lawyer, I have been informed and understand that certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims.

28. I am informed that a patent claim may be written in “independent” or “dependent” form. I am informed that a dependent claim encompasses all the elements or steps of the claim or claims from which it depends.

29. I am informed that a claimed invention of a patent may be unpatentable as “anticipated” or as “obvious” in view of prior art.

30. I am informed that, to anticipate a claim, a prior art reference must teach every element or step of the claim. If a reference is silent about a claimed feature or step, it may still disclose it inherently if the missing feature would have been recognized as necessarily present in what the reference discloses.

A. Obviousness Generally

31. I am informed and understand that a patent claim is not patentable if the differences between the patent claim and the prior art are such that the claimed subject matter as a whole would have been obvious at the time the claimed invention was made to a person having ordinary skill in the relevant art (“POSA”) at the time of the invention.

1. The POSA Requirement

32. I have been informed that a POSA is a hypothetical person who is presumed to be aware of all pertinent prior art, thinks along conventional wisdom in the art, and is a person of ordinary creativity.

33. I have been informed that when determining the level of ordinary skill in the art, the factors to consider include: (1) the level of education and experience of persons actively working in the field at the relevant time, (2) the types of problems encountered in the art at the relevant time, and (3) the sophistication of the technology in the art at the relevant time, including how quickly innovations were made in the art at the relevant time.

34. I have been informed that the time of the invention is the effective filing date of the patent application that eventually issued as the '658 Patent, i.e., March 6, 2000. Unless otherwise stated, my testimony herein refers to the knowledge of POSA as of March 6, 2000.

2. The Obviousness Inquiry

35. Obviousness, as I have been informed, is based on (1) the scope and content of the prior art, (2) the differences between the prior art and the claim, (3) the level of ordinary skill in the art, and, (4) to the extent that they exist, certain objective indicia of non-obviousness (which may also be referred to as “secondary considerations” of non-obviousness).

36. I have been informed that whether there are any relevant differences between the prior art and the claimed invention is to be analyzed from the view of a POSA at the time of the invention. As such, my opinions as to a POSA are as of the time of the invention, even if not expressly stated as such; for example, even if stated in the present tense.

37. I have been informed that a claimed invention may have been obvious based on a single prior art reference or multiple prior art references. I have also been informed that a POSA often will be able to fit the teachings of multiple references together like pieces of a puzzle, and that familiar items may have obvious uses beyond their primary purposes. Further, I have been informed that the law permits the application of “common sense” in examining whether a claimed invention would have been obvious to a POSA.

38. In analyzing the relevance of the differences between the claimed invention and the prior art, I have been informed that I must consider the impact, if

any, of such differences on the obviousness or non-obviousness of the invention as a whole, not merely some portion of it. The person of ordinary skill faced with a problem is able to apply his or her experience and ability to solve the problem and also look to any available prior art to help solve the problem.

39. I have been informed that a precise teaching in the prior art directed to the subject matter of the claimed invention is not needed. I have been informed that combining the teachings of prior art references does not require combining specific structures of those references. I have been informed that one may take into account the inferences and creative steps that a POSA would have employed in reviewing the prior art at the time of the invention. For example, if the claimed invention combined elements known in the prior art and the combination yielded results that were predictable to a POSA at the time of the invention, then this evidence would make it more likely that the claim was obvious. On the other hand, if the combination of known elements yielded unexpected or unpredictable results, or if the prior art teaches away from combining the known elements, then this evidence would make it more likely that the claim that successfully combined those elements was not obvious.

40. I have been informed that there are recognized, exemplary, rationales for combining or modifying references to show obviousness of claimed subject matter. Some of the rationales include the following:

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

41. I am informed that a POSA does not need to have the same reason to combine references that inspired the inventor of the claimed invention.

42. I have been informed that a reference may “teach away” from its

combination with another reference. I have been informed that a reference may be considered to teach away from its combination with another reference when a POSA 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 in the claimed invention. For example, a reference teaches away from a combination with another reference when the proposed combination would not have worked for its intended purpose. However, I have been informed that a reference does not teach away by merely expressing a preference for an alternative without criticizing, discrediting, or otherwise discouraging investigation into the claimed invention.

B. Analogous Art

43. I have been informed that a prior art reference must be “analogous art” to the claimed invention in order for it to be used for an obviousness analysis. I have also been informed that prior art is analogous if (1) the reference is from the same field of endeavor as the claimed invention, regardless of the problem addressed, or (2) even if the reference is not within the field of the inventor’s endeavor, the reference is reasonably pertinent to the problem faced by the inventor. I have been informed that to be “reasonably pertinent,” the problems to which the claimed invention and the reference must be identified and compared from the perspective of a POSA who is considering turning to the teachings of references outside his or her field of endeavor.

44. The '658 Patent relates to user authentication. Under the “Field of the Invention,” the '658 Patent provides: “This invention relates generally 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.” Ex-1001, 1:6-11. As I discuss herein, the prior art references Sormunen and Perlman are from the same field of endeavor as the claimed invention of the '658 Patent.

C. Objective Indicia of Nonobviousness

45. I have been informed that objective indicia can be important evidence regarding whether a patent is obvious or nonobvious. However, objective indicia must have an appropriate nexus to the claimed invention. I have been informed that having an appropriate nexus means that the objective indicia is a result of the merits of a claimed invention (rather than the result of design needs, market-pressure, advertising, or similar activities). Such indicia include: (a) commercial success of products covered by the patent claims; a long-felt need for the invention; failed attempts by others to make the invention; copying of the invention by others in the field; unexpected results achieved by the invention as compared to the closest prior art; praise of the invention by the infringer or others in the field; the taking of licenses under the patent by others; expressions of surprise by experts and those skilled in the art at the making of the invention; and the patentee proceeded contrary to the

accepted wisdom of the prior art.

46. To the extent Patent Owner identifies any objective indicia of non-obviousness, I may address them in a subsequent report.

V. The Level of Ordinary Skill in the Art

47. I have been informed that the level of ordinary skill in the art is based on factors: (1) the level of education and experience of persons actively working in the field at the relevant time, (2) the types of problems encountered in the art at the relevant time, and (3) the sophistication of the technology in the art at the relevant time, including how quickly innovations were made in the art at the relevant time. Based on my education and experience, I understand and know the capabilities of a POSA as of March 6, 2000.

48. It is my opinion that a POSA at the time of the invention would have had a bachelor's degree in computer science, management of information systems, or electrical engineering, or similar field, with one-to-two years of experience in the design, support, or implementation of systems requiring user authentication. Additional education may substitute for experience with user authentication. Likewise, additional relevant experience with user authentication may substitute for education.

49. My qualifications exceeded those of a POSA as of March 6, 2000. However, my analysis is based on the perspective of a POSA.

VI. The '658 Patent

A. Summary

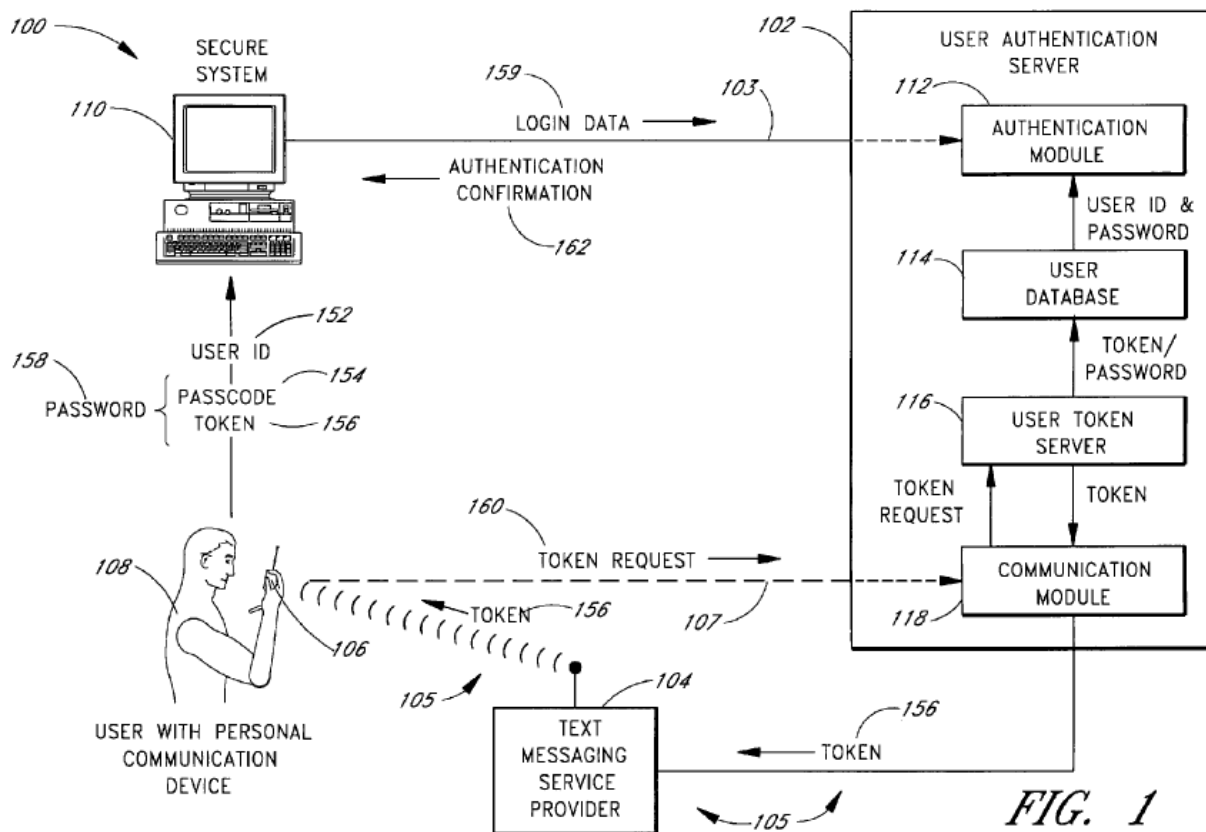
50. The '658 Patent is titled "Use of Personal Communication Devices for User Authentication," and issued from Application No. 09/519,829, filed on March 6, 2000. Ex-1001, Cover. The '658 Patent relates "generally to the authentication of users of secure systems and, more particularly . . . to a system through which user tokens required for user authentication are supplied through personal communication devices such as mobile telephones and pagers." Ex-1001, 1:7-11.

51. The '658 Patent notes that systems "typically require the submission of a user ID and password combination" for access. Ex-1001, 1:15-20. The '658 Patent provides that "[p]asswords created by users are often combinations of words and names, which are easy to remember but also easily guessed." Ex-1001, 1:28-38. The '658 Patent notes that "[g]uessing passwords is a frequent technique used by 'hackers' to break into systems." Ex-1001, 1:29-30. As a consequence, "many systems impose regulations on password formats that require mixtures of letters of different cases and symbols and that no part of a password be a word in the dictionary." Ex-1001, 1:31-34. However, complex or frequently changed passwords often "results in the password being written down." Ex-1001, 1:35-38.

52. The '658 Patent notes that "requiring a two-factor authentication process" was a known solution. Ex-1001, 1:44-46. The '658 Patent notes that the

SecurID product was a currently used for “a two-factor authentication process,” but it “requires users to carry an additional item on their person in order to access a secure system.” Ex-1001, 1:54-56. The ’658 Patent notes that, as of March 6, 2000, “many users already carry[] a personal communication device such as mobile phones or pagers.” Ex-1001, 1:57-60. The ’658 Patent asserts that it would therefore be convenient to use mobile phones or pagers for two-factor authentication instead of carrying a separate device (e.g., the RSA SecurID card). Ex-1001, 1:54-59.

53. The ’658 Patent discloses “a password setting system for setting user passwords for a secure system, such as a computer system or a secure area of a building.” Ex-1001, 1:63-66. FIG. 1 of the ’658 Patent depicts “user authentication system 100 according to a preferred embodiment of the present invention.” Ex-1001, 4:2-4.



Ex-1001, FIG. 1.

54. The '658 Patent provides that “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**.” Ex-1001, 2:11-15. The '658 Patent discloses that the RSA SecurID product required a “user passcode or personal identification number” (PIN) as the “first factor” in two-factor authentication. Ex-1001, 1:46-47. For the second factor, the SecurID card possessed by the user “generates and displays unpredictable, one-time-only access codes that automatically change every 60 seconds.” Ex-1001, 1:47-50. The “one-time-only”

code can be used for “logging into a system.” Ex-1001, 1:51-53.

55. Instead of entering the passcode or PIN from a code generator to get a random code, the ’658 Patent discloses requesting the code through a phone call or text, or through a user interface. Ex-1001, FIG. 3 at 302, 6:28-47.

56. The ’658 Patent refers to this as the “token.” The requesting personal communication device is identified as a user’s device because of an association of the user ID with the phone number, which can be stored in “any database capable of storing user ID and password data.” Ex-1001, 2:33-35, 5:20-21.

57. The ’658 Patent discloses that a “token” is generated by “any number of methods that preferably produces a random or pseudorandom sequence of numbers and/or digits.” Ex-1001, 6:53-55. This “token” is then sent to the personal communication device, and may be time-limited. Ex-1001, 4:42-45, 9:61-54.

58. The disclosed password-setting system of the ’658 Patent generates a password based on the passcode and token. Ex-1001, 9:28-30. The password is “preferably generated by concatenating the passcode 154 and the token 156.” Ex-1001, 9:31-32. For example, the ’658 Patent discloses a passcode of “abcd” and a token of “1234,” and the password being “abcd1234.” Ex-1001, 4:52-56. The ’658 Patent also discloses that the passcode can be “null, in which case the token 156 alone is used as the password 158.” Ex-1001, 4:61-65. The ’658 Patent discloses that in the preferred embodiment, the user enters the password in a login screen, as

shown in FIG. 2A. Ex-1001, 4:52-63. Alternatively, the user enters the passcode and token separately, as shown in FIG. 2B. Ex-1001, 4:52-63.

59. The user is able to access the secure system by “logging in using the supplied token 156.” Ex-1001, 9:55-60. The user uses it for logging in by submitting it along with the user’s passcode (e.g., FIG. 2B), or by concatenating the passcode and token to form a “password” (e.g., FIG. 2A). Ex-1001, 5:8-10 (“authenticating a user based upon a supplied user ID 152 supplemented by a supplied password 158 or a passcode 154 and a token 156 combination”), 7:42-45, 9:54-60 (“The user 108 preferably concatenates his memorized secret passcode 154 with the valid token 156 to create the password 158.”).

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

Ex-1001, FIGs. 2A and 2B.

60. The '658 Patent discloses “modules” of a “user authentication sever.”

Ex-1001, 5:1-6:24. For example, the '658 Patent discloses a “control module,” with functions including user account and password generation. Ex-1001, 8:53-9:64. In yet another example, the '658 Patent discloses a “communication module,” with functions including receiving requests for tokens and sending responses to requests for tokens. The '658 Patent discloses that the communication module may be, for example, a mobile phone with SMS capability, an ISDN card or an X.25 connection card connected to an SMS gateway of a mobile phone service provider, a phone dialer, or an automated telephone response system with caller ID. Ex-1001, 10:14-41, 11:11-15. Finally, the '658 Patent discloses an “authentication module,” which receives and responds to requests sent over the secure computer network. Ex-1001, 5:1-18. The '658 Patent provides:

The authentication module 112 is preferably identical to the code or software provided with operating systems such as Windows NT that authenticates users upon login. In alternative embodiments, the authentication module 112 may be any code, device, or module capable of authenticating a user based upon a supplied user ID 152 supplemented by a supplied password 158 or a passcode 154 and a token 156 combination.

Ex-1001, 5:3-10. Regarding the modules, the '658 Patent provides: “The various modules and components of the user token server 116 are described herein from a functional perspective. The various functional components may, however, be

seamlessly integrated into one or more executable programs, data structures, and/or physical components.” Ex-1001, 8:10-15.

61. The '658 Patent has seven claims. Claims 1 and 5 are independent claims. Claims 2-4 depend from claim 1 and claims 6-7 depend from claim 5.

B. Prosecution History

62. The application from which the '658 Patent issued, U.S. Patent Application No. 09/519,829 (“the '829 application”), was filed on March 6, 2000. At the time it was filed, it included 27 claims. Ex-1002, 69-71.

63. On March 21, 2001, a preliminary amendment was filed which cancelled all original 27 claims and presented 26 new claims (numbered 28-53). Ex-1002, 154-160. The first independent claim following the preliminary amendment—claim 28—is reproduced below.

28. A method of authenticating a user, the method comprising:
 associating the user with a personal communication device possessed by the user;
 generating 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;
 setting a password associated with the user to be the new password;
 transmitting the token to the personal communication device; and
 receiving the password from the user.

Ex-1002, 157.

64. The '829 application received a first non-final rejection on December 15, 2003. Ex-1002, 181-187. Claims 37-39 were rejected as anticipated by

Australian Patent Application No. 63545/98 by Schmitz. Ex-1002, 184. Additionally, claims 28-36 and 40-53 were rejected as obvious over Schmitz in view of the Handbook of Applied Cryptography by Menezes. Ex-1002, 185-86. The examiner identified that “it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the system disclosed by Schmitz by creating a password using the user’s password information in addition to an ID for the device (the token), using a hashing function, as disclosed by Menezes, in order to make dictionary attacks less effective.” Ex-1002, 186.

65. In response, the applicants argued that Schmitz makes and receives a request from the same device and that Schmitz does not teach associating a user with a personal communication device possessed by the user. Ex-1002, 234-239. There were no substantive claim amendments in this response.

66. Claims 28-31 and 43-53 were rejected again on May 24, 2004, as anticipated by U.S. Patent No. 5,323,146 to Glaschick. Ex-1002, 245. Claims 37-39 were rejected as anticipated by U.S. Patent No. 6,226,364 to O’Neil. Ex-1002, 245-246. Claims 32-36 and 40-42 were rejected as obvious over O’Neil and Glaschick. See Ex-1002, 242-248. The examiner found a motivation to combine O’Neil and Glaschick “in order to prevent a privileged user from acquiring the password of a user by reading it form [sic] the memory.” Ex-1002, 247.

67. In response, the applicants argued that Glaschick failed to disclose

“associating the user with a personal communication device possessed by the user,”
“wherein the request is transmitted from a personal communication device,” and
“transmitting the token to the personal communication device.” Ex-1002, 258-260.
The applicants also argued that there was no teaching, suggestion, or motivation to
combine Glaschick with O’Neil. Ex-1002, 262-263.

68. All claims were rejected again on February 7, 2005, in a final rejection
that maintained the rejections based on Glaschick and O’Neil. Ex-1002, 266-274.
The examiner found: “[T]he data station as disclosed by Glaschick may be a
computer with programs (see column 1, line 15), and clearly has communication
capability. Applicant’s personal communication device, as viewed in light of
Applicant’s specification, is simply a type of computer with programs; therefore, the
claimed invention is anticipated.” Ex-1002, 271. Regarding combining Glaschick
with O’Neil for obviousness, the examiner further found that “one skilled in the art
would recognize that the motivation supplied by Glaschick would apply to *any*
computerized system having authentication.” Ex-1002, 272-273.

69. Following an examiner’s interview (Ex-1002, 276-277), the applicant
amended the claims to overcome the final rejection (Ex-1002, 280-285). The
amendments to independent claim 28 (issued claim 1) are reproduced below.

Listing of Claims

Claims 1-27 (Canceled)

Claim 28 (Currently amended): 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:

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;

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

generating a new password for said first secure computer network based at least upon [[a]] the token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user;

setting a password associated with the user to be the new password;

activating access the user account on the first secure computer network;

transmitting the token to the personal communication device; [[and]]

receiving the password from the user via the first secure computer network; and

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.

Ex-1002, 281.

70. Following the amendments to the claims (including cancellation of claims 30-31 and 37-53), a notice of allowance was issued on August 8, 2005. Ex-1002, 289-296. The examiner's "statement of reasons for allowance" was that "no art could be found wherein **the transaction for determining the password** in setting up of a new calling-card-derived temporary network account **is performed entirely over a connection other than that used by [the] eventual network account.**" Ex-1002, 294-95. The examiner also found: "Some of the closest art, the 'Monkey Technical Overview' (see IDS filed 23 May 2000), sets up a password for

a temporary account, **but the user request is sent over the network account connection.**” Ex-1002, 295.

71. The “Monkey Technical Overview,” dated July 25, 1999 (Ex-1002, 94-99) discloses:

1. Introduction

The mobile network key ("monkey") is a one-time password system for secure two-factor "what you have and what you know" user authentication. In contrast to other hardware-based solutions, which depend on their own proprietary infrastructure to be established - by handing a hardware authentication token to each user -, monkey employs an existing world-wide infrastructure, the global GSM network for digital mobile telephony, and thus turns any GSM mobile telephone into an authentication token. Every GSM telephone is capable of receiving and displaying short messages.

monkey makes use of this GSM service to efficiently transmit one-time passwords via a separate channel, i.e. the GSM network, to users requesting authentication. Suppose Alice would like to authenticate herself. To do so, she initiates a connection to the point of authentication, e.g. a telnet session to a firewall machine. After her having identified herself by means of a user name and, at the discretion of her security administrator, a fixed password, a temporary one-time password, transmitted by monkey, appears on the display of her mobile phone. Alice reads the password off the display, types it in and, in case she performed well, is granted access.

72. The Monkey Technical Overview further discloses the use of an “authentication server consist[ing] of four different kinds of modules which are at runtime instantiated as processes”: a “user database modules,” “SMS transmission modules,” “authentication modules,” and “log modules.” Ex-1002, 97-98.

7. monkey implementation

The monkey authentication server consists of four different kinds of modules which are at runtime instantiated as processes. [\[top\]](#)

a. User database modules

These modules handle the mapping from user names to the corresponding mobile phone numbers by performing a lookup in the user database. monkey currently includes user database modules for accessing database management systems via LDAP, SQL and ODBC (Windows NT only), and for highly efficient indexed flat file user databases. Aiming at compatibility, monkey is designed to integrate with an existing database infrastructure, instead of maintaining a separate dedicated database of monkey users. [\[top\]](#)

b. SMS transmission modules

They are responsible for transmitting a given short message to a specified mobile phone number. The Siemens "M" family of GSM modules, which basically consists of stationary mobile phones that can be attached to the serial interface of a computer, as well as potentially any other GSM module that adheres to the standard for GSM AT commands, are currently supported for low-bandwidth applications, as is UCP via a dedicated X.25 link for a direct high-bandwidth connection to a GSM short message service center. Load balancing to evenly distribute the SMS traffic over several channels in order to increase the total bandwidth available for SMS transfers in high-end scenarios is implemented as well. [\[top\]](#)

c. Authentication modules

These modules maintain the link between monkey and the authentication clients. On incoming requests, they generate the one-time passwords, ask the user database modules to find the phone number of the user to be authenticated, form a short message containing the generated password and transmit the short message by passing it to one of the SMS transmission modules. As of this writing, the RADIUS

Internet standard is the authentication protocol employed. For electronic commerce applications an additional proprietary protocol has been developed, which is capable of transferring encrypted billing information to the monkey server. Moreover, a module exists that integrates with the authentication services of the B2 certified version of Data General's DG/UX. [\[top\]](#)

73. Thus, as the examiner indicated, the Monkey Technical Overview discloses authenticating a user through the use of a “fixed password” the user knows and a “one-time password” generated in response to a user request. The Monkey Technical Overview also discloses having a database of users and their mobile phone numbers. However, as indicated by the examiner, while the Monkey Technical Overview discloses that the response to the user’s request is sent via a separate cell phone network, the user’s request was not. Instead, the user’s request is submitted through the telnet session to the firewall machine (the “network account connection”).

C. Priority Date of Claims

74. For the purpose of this *inter partes* review, I have been instructed to

assume that the effective filing date of each of the Challenged Claims is no earlier than March 6, 2000, the filing date of the '658 Patent.

VII. State of the Art

75. As I discussed above, the '658 Patent concerns two-factor authentication, the use of communication networks in a user authentication process, and the process of generating passwords.

A. Two-Factor Authentication

76. The use of two-factor authentication was well-known by March 6, 2000. For example, as the '658 Patent acknowledges, it was already used with the RSA SecurID card—a commercial product in widespread use and distribution. Ex-1001, 1:44-53. The idea that two-factor authentication could be based on something you know (a password or PIN) and something you have” was well-established. Ex-1002, 85 (“RSA SecurID two-factor Authentication is based on something you *know* (a password or PIN), and something you *have* (an authenticator) – providing a much more reliable level of user authentication than reusable passwords.”).

77. The use of a mobile device as the “what you have” is shown in The Monkey Technical Overview (Ex-1002, 94-99), which discloses “a one-time password system for secure two-factor ‘what you have and what you know’ user authentication.” Instead of “handing a hardware authentication token to each user,” it discloses “turn[ing] any GSM mobile telephone into an authentication token.” Ex-

1. Introduction

The mobile network key ("monkey") is a one-time password system for secure two-factor "what you have and what you know" user authentication. In contrast to other hardware-based solutions, which depend on their own proprietary infrastructure to be established - by handing a hardware authentication token to each user -, monkey employs an existing world-wide infrastructure, the global GSM network for digital mobile telephony, and thus turns any GSM mobile telephone into an authentication token. Every GSM telephone is capable of receiving and displaying short messages.

monkey makes use of this GSM service to efficiently transmit one-time passwords via a separate channel, i.e. the GSM network, to users requesting authentication. Suppose Alice would like to authenticate herself. To do so, she initiates a connection to the point of authentication, e.g. a telnet session to a firewall machine. After her having identified herself by means of a user name and, at the discretion of her security administrator, a fixed password, a temporary one-time password, transmitted by monkey, appears on the display of her mobile phone. Alice reads the password off the display, types it in and, in case she performed well, is granted access.

Ex-1002, 94.

78. U.S. Patent No. 6,173,400 to Radia J. Perlman, et al. ("Perlman," Ex-1005), has a filing date of July 31, 1998. Perlman recognizes:

Many users currently rely on authentication tokens to provide an additional level of user authentication based on "something you have" (versus "something you know", like a password). Authentication tokens are physical devices that people carry while passwords are simply remembered. There are a variety of authentication tokens currently available in the marketplace. These authentication tokens include time-synchronized authentication tokens, challenge response authentication tokens, and smart cards.

Ex-1005, 1:38-46.

79. The use of something private (something “secret”) and something public (i.e., shared with others) was also common.

80. Thus, authentication using “secret information known to the user” and “information provided to the user through an object possessed by the user” was well-known by March 6, 2000. Ex-1001, 2:11-15.

B. The Use of Different Communication Networks

81. By March 6, 2000, the use of independent communication networks as part of the authentication process was well-known. For example, U.S. Patent No. 5,881,226 to Brian Veneklasé (“Veneklasé,” Ex-1007) was filed on October 28, 1996. Veneklasé discloses the use of secret second channel or communications medium to enhance security. Veneklasé relates to a “security and/or access restriction system which is adapted to grant only authorized users access to a computer system and/or to certain data which may be resident within the computer system and/or resident within a communications channel and/or other communications medium.” Ex-1007, 1:4-10. Veneklasé discloses an authentication system that includes a means for receiving a password on a first communication channel for generating a code for use on a second communications channel, and only allowing individual access to the system if the individual generates and communicates the code to the code generation means. Ex-1007, 3:20-31. Veneklasé

discloses “the use of a ‘secret’ password, a ‘secret’ substantially random number, and a ‘secret’ second channel allows for multiple levels of security before access to the computer system is achieved and provides enhanced security over the prior art.” Ex-1007, 6:16-20. Veneklasen discloses that this is achieved using “substantially ‘off the shelf’ and readily available components.” Ex-1007, 6:14-16. Veneklasen directly shows using one channel to request and receive a token that will then be used on a different channel to provide authentication.

C. The Use of Cell Phones and Pagers for Two-Factor Authentication

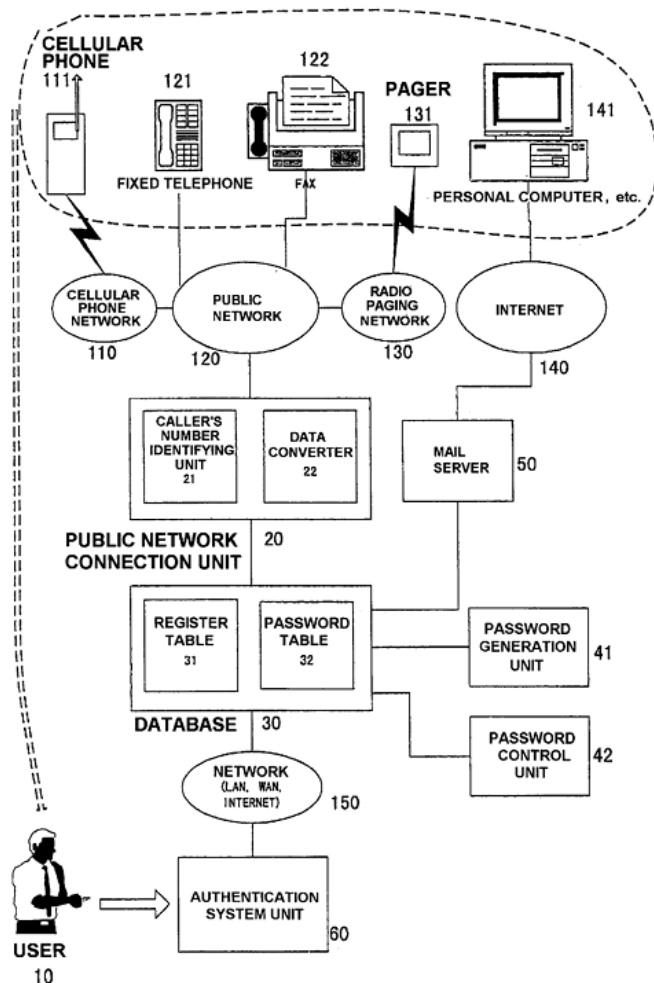
82. By March 6, 2000, it was well-known to communicate with users using cellular telephones (and cellular networks) for user authentication.

83. For example, U.S. Patent No. 6,731,731 to Yasushi Ueshima (“Ueshima,” Ex-1006) claims priority to a Japanese patent application filed on July 30, 1999. Ueshima “relates to CTI (computer telephony integration) and, particularly, to user authentication utilizing CTI.” Ex-1006, 1:15-17. Ueshima discloses registering the user’s information in a database, including their name and telephone number. Ex-1006, 12:50-13:12. Ueshima discloses a user authentication process of associating a user with a telephone number, receiving a call from the user, authenticating the user based on the telephone number from which he or she is calling, generating a password for the authenticated user, sending it to the user, and using the generated password to access a secured network that is different from the

telephone communications channel. Ex-1006, 3:30-65.

84. FIG. 1 of Ueshima is reproduced below.

FIG. 1



Ex-1006, Fig. 1

85. By 2000, it was well known to use mobile phones and/or pagers to receive tokens/passwords used to access secure networks. For example, The Monkey Technical Overview (Ex-1002, 94-99) discloses using “GSM service to efficiently transmit one-time passwords via a separate channel, i.e. the GSM

network, to users requesting authentication.”

1. Introduction

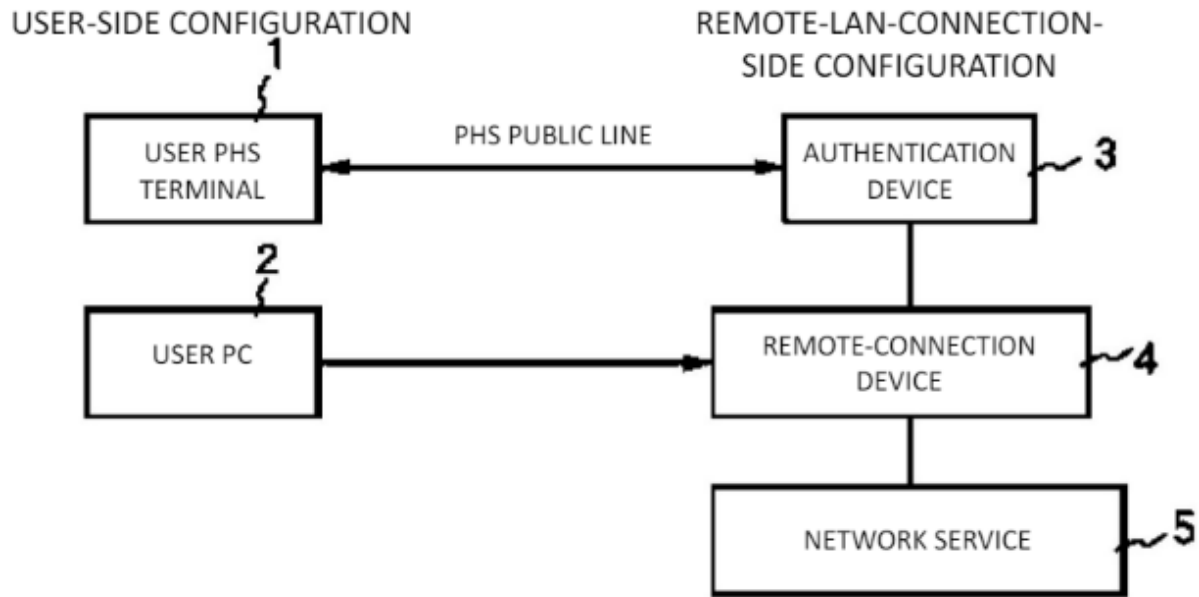
The mobile network key ("monkey") is a one-time password system for secure two-factor "what you have and what you know" user authentication. In contrast to other hardware-based solutions, which depend on their own proprietary infrastructure to be established - by handing a hardware authentication token to each user -, monkey employs an existing world-wide infrastructure, the global GSM network for digital mobile telephony, and thus turns any GSM mobile telephone into an authentication token. Every GSM telephone is capable of receiving and displaying short messages.

monkey makes use of this GSM service to efficiently transmit one-time passwords via a separate channel, i.e. the GSM network, to users requesting authentication. Suppose Alice would like to authenticate herself. To do so, she initiates a connection to the point of authentication, e.g. a telnet session to a firewall machine. After her having identified herself by means of a user name and, at the discretion of her security administrator, a fixed password, a temporary one-time password, transmitted by monkey, appears on the display of her mobile phone. Alice reads the password off the display, types it in and, in case she performed well, is granted access.

Ex-1002, 94.

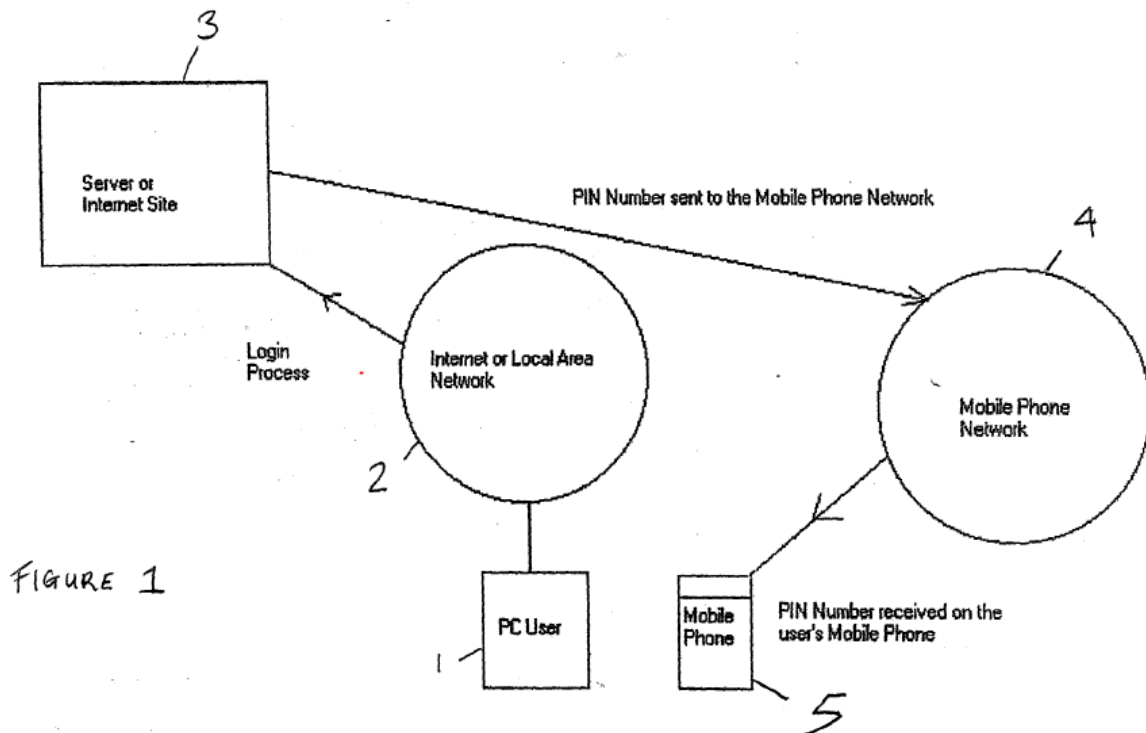
86. Another example is Japanese Patent Application No. H10-178410, filed June 25, 1998 ("Katou," Ex-1008) "relates to an authentication system and an authentication device." Ex-1008, [0001]. Katou discloses receiving a token/password upon authentication with a mobile or pager number. As shown in FIG. 1 of Katou below, Katou discloses the use of a "commercially available simplified, mobile-telephone terminal, such as a [Personal Handy-phone System (PHS)] terminal." Ex-1008, [0025].

FIG. 1



Ex-1008, FIG 1.

87. European Patent Publication No. EP 1107089 (“Williamson,” Ex-1009) arises from a Great Britain patent application filed December 11, 1999. Williamson discloses “a method of obtaining strong authentication for a remote network, by way of the remote network generating a security code, and transmitting this code to a user, via a separate connection (for example, via a mobile telephone). This security code being used by the user to gain access to the remote network.” Ex-1009, Cover (57). Figure 1 of Williamson is reproduced below.



Ex-1009, Figure 1.

88. Williamson discloses that “[a] security token is conventionally a device by which means a user can prove to the remote network site which they wish to access their identity. Strong authentication requires the combination of a username, password and a security token, and is used when authentication by means of a username and password alone is not sufficient for security purposes.” Ex-1009, [0001]. Williamson discloses that conventional security token devices are typically “specialized devices,” “often expensive,” “difficult to use,” and may “be lost or damaged.” Ex-1009, [0002]. Williamson proposes using a mobile phone or pager instead. Ex-1009, [0003]. A user uses a terminal-type device 1 (e.g., “PC or workstation”) to connect to “remote/server/host 3 via a network 2 (for example, a

LAN, WAN or an internet site).” Ex-1009, [0013]. The user submits a password and username which is associated with a telephone number corresponding to the user’s telecommunication device 5. Ex-1009, [0014]. The server 3 sends a “one-time use PIN” via the “telecommunication network 4 to the telecommunications device 5, for example, as a text message,” and the user enters it via terminal 1 to be authenticated. Ex-1009, [0015]-[0016]. “The telecommunications device 5, thus acts as a ‘security token’ to prove the user’s identity and authorize the user’s access to the remote server/host.” Ex-1009, [0016].

D. Concatenation for Passwords

89. It was also well known by March 6, 2000, that a password could be formed by concatenation. A password could be combined or concatenated with additional user information to strengthen the overall security of the system. For example, Perlman discloses concatenating a character string generated by an authentication token with an already-known PIN to establish a shared secret between a workstation and a server. Ex-1005, 8:14-23, 8:55-9:9.

90. As another example, U.S. Patent No. 5,787,169 to Eldridge (“Eldridge,” Ex-1010) discloses accessing encrypted files in a secured system by concatenating a password with a salt value, where the resultant string is hashed and compared to an independently computed value for access. Ex. 1010, [0030]-[0032]. Further, Menezes identifies that a password can be augmented with a string, which

can be a user ID (i.e., user information). Ex-1002 at 218.

91. A POSA at the time of the '658 Patent (May 6, 2000) would have been knowledgeable about strings and concatenation. This is shown, for example, by textbooks that were used to teach Computer Science courses in the late 1980s.

92. Shown below are examples of both the theory and the practice regarding concatenation. The theory is that of programming languages and programming concepts that computer science students were exposed to. The practice (or implementation) of the theory is provided as inclusions in computer programming languages and normal usage when writing programs. The cited texts are, in my opinion, foundational and representative references that a POSA would have either personally used or would have at least been aware of.

93. Strings are such a fundamental part of programming languages that they are the **very first** topic explored in Section 1.1 on page 1 of an automata theory reference used for undergraduate computer science study, including discussion of concatenation:

1.1 STRINGS, ALPHABETS, AND LANGUAGES

A “symbol” is an abstract entity that we shall not define formally, just as “point” and “line” are not defined in geometry. Letters and digits are examples of frequently used symbols. A *string* (or *word*) is a finite sequence of symbols juxtaposed. For example, a , b , and c are symbols and $abcb$ is a string. The *length* of a string w , denoted $|w|$, is the number of symbols composing the string. For example, $abcb$ has length 4. The empty string, denoted by ϵ , is the string consisting of zero symbols. Thus $|\epsilon| = 0$.

A *prefix* of a string is any number of leading symbols of that string, and a *suffix* is any number of trailing symbols. For example, string abc has prefixes ϵ , a , ab , and abc ; its suffixes are ϵ , c , bc , and abc . A prefix or suffix of a string, other than the string itself, is called a *proper* prefix or suffix.

The *concatenation* of two strings is the string formed by writing the first, followed by the second, with no intervening space. For example, the concatenation of *dog* and *house* is *doghouse*. Juxtaposition is used as the concatenation operator. That is, if w and x are strings, then wx is the concatenation of these two

Ex-1011, 1.

94. As taught by Hopcroft & Ullman: “A *string* (or *word*) is a finite sequence of symbols juxtaposed. For example, a , b , and c are symbols and $abcb$ is a string.” Further: “The concatenation of two strings is the string formed by writing the first, followed by the second, with no intervening space. For example, the concatenation of *dog* and *house* is *doghouse*.” Ex-1011, 1.

95. In another foundational undergraduate text, Ghezzi & Jazayeri, discusses strings as they relate to a range of programming languages (e.g., PL1, Ada, Pascal, or C). Ex-1012. Specifically, it provides that concatenation was a conventional string operation.

Strings provide a well-known example of sequences in which the component type is character. The concept of sequence also captures the familiar data-processing idea of a sequential *file*.

It is difficult to abstract a common behavior from the examples of sequences provided by existing programming languages. For example, SNOBOL4 views strings as data objects with a rich set of operations. Conversely, Pascal and C view strings simply as arrays of characters, with no special primitives for string manipulation. Taking somewhat of a middle ground, PL/I and Ada provide string manipulation primitives but, to reduce the problem of dynamic storage allocation, require that the maximum size of a string be specified in the declaration of the string. Files present more serious problems in that they often have peculiar, system-dependent aspects as a result of the necessary interface with the operating system.

Conventional operators on strings include the following.

1. *Concatenation*. The concatenation of *THIS_IS_* and *AN_EXAMPLE* gives *THIS_IS_AN_EXAMPLE*.

Ex-1012, 101.

96. *Algorithms* by Robert Sedgewick was another textbook for undergraduate computer science. Sedgewick discusses “Concatenation” as a fundamental operation of describing patterns:

Describing Patterns

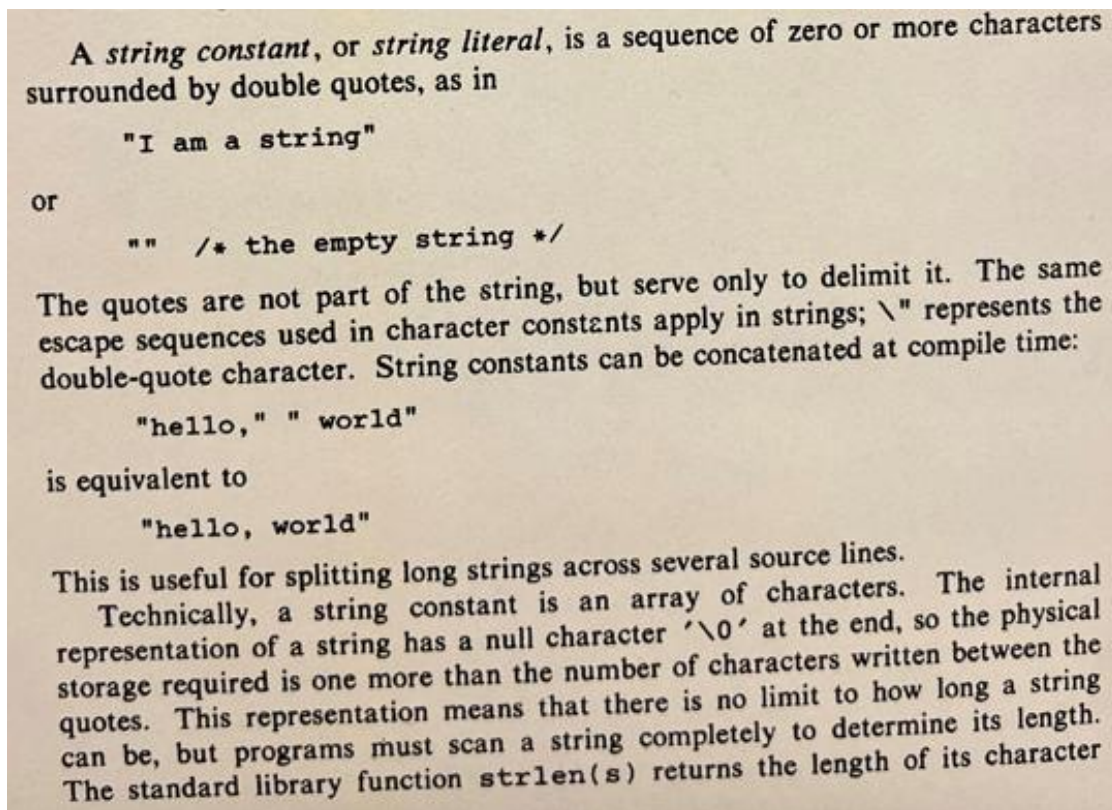
We'll consider pattern descriptions made up of symbols tied together with the following three fundamental operations.

- (i) *Concatenation*. This is the operation used in the last chapter. If two characters are adjacent in the pattern, then there is a match if and only if the same two characters are adjacent in the text. For example, AB means A followed by B.

Ex-1013, 258.

97. Apart from theory, the implementation and use of concatenation was, as of March 6, 2000, quite basic and prolific. Almost all high-level languages (both compiled and interpreted) have the concept of strings (and did as of March 6, 2000).

As an example, I selected the C programming language. C was in widespread use well before March 6, 2000.⁶ The C programming language was created by Dennis Ritchie in the 1970s, and remains very widely taught and used. Ritchie coauthored a reference for C with Brian Kernighan. Ex-1014. Kernighan and Ritchie (“K&R”) discuss the concept of strings and string concatenation:



A *string constant*, or *string literal*, is a sequence of zero or more characters surrounded by double quotes, as in

```
"I am a string"
```

or

```
"" /* the empty string */
```

The quotes are not part of the string, but serve only to delimit it. The same escape sequences used in character constants apply in strings; \" represents the double-quote character. String constants can be concatenated at compile time:

```
"hello," " world"
```

is equivalent to

```
"hello, world"
```

This is useful for splitting long strings across several source lines.

Technically, a string constant is an array of characters. The internal representation of a string has a null character '\0' at the end, so the physical storage required is one more than the number of characters written between the quotes. This representation means that there is no limit to how long a string can be, but programs must scan a string completely to determine its length. The standard library function `strlen(s)` returns the length of its character

Ex-1014 at 38.

98. K&R also provide the code for a string concatenation function:

⁶ An example of this is shown by the Monkey Technical Overview: “The monkey architecture clings to the maxim ‘keep it simple’, which has resulted in a straightforward and comprehensible server design in hardly more than 10,000 lines of C code.” Ex-1002, 95.

As a third example, consider the standard function `strcat(s,t)`, which concatenates the string `t` to the end of the string `s`. `strcat` assumes that there is enough space in `s` to hold the combination. As we have written it, `strcat` returns no value; the standard library version returns a pointer to the resulting string.

```
/* strcat: concatenate t to end of s; s must be big enough */
void strcat(char s[], char t[])
{
    int i, j;

    i = j = 0;
    while (s[i] != '\0')    /* find end of s */
        i++;
    while ((s[i++] = t[j++]) != '\0')    /* copy t */
        ;
}
```

As each character is copied from `t` to `s`, the postfix `++` is applied to both `i` and `j` to make sure that they are in position for the next pass through the loop.

Ex-1014 at 47-48.

99. Concatenation was so common that there was an implementation of the function included with the language. Above, K&R refer to the “standard library version.” The specific standard library concatenation functions are listed in Section 7.8 “Miscellaneous Functions”:

7.8 Miscellaneous Functions

The standard library provides a wide variety of functions. This section is a brief synopsis of the most useful. More details and many other functions can be found in Appendix B.

7.8.1 String Operations

We have already mentioned the string functions `strlen`, `strcpy`, `strcat`, and `strcmp`, found in `<string.h>`. In the following, `s` and `t` are `char *`'s, and `c` and `n` are `ints`.

<code>strcat(s,t)</code>	concatenate <code>t</code> to end of <code>s</code>
<code>strncat(s,t,n)</code>	concatenate <code>n</code> characters of <code>t</code> to end of <code>s</code>
<code>strcmp(s,t)</code>	return negative, zero, or positive for <code>s < t</code> , <code>s == t</code> , or <code>s > t</code>
<code>strncmp(s,t,n)</code>	same as <code>strcmp</code> but only in first <code>n</code> characters
<code>strcpy(s,t)</code>	copy <code>t</code> to <code>s</code>
<code>strncpy(s,t,n)</code>	copy at most <code>n</code> characters of <code>t</code> to <code>s</code>
<code>strlen(s)</code>	return length of <code>s</code>
<code>strchr(s,c)</code>	return pointer to first <code>c</code> in <code>s</code> , or <code>NULL</code> if not present
<code>strrchr(s,c)</code>	return pointer to last <code>c</code> in <code>s</code> , or <code>NULL</code> if not present

Ex-1014, 166.

100. Since these concepts were (and still are) addressed early in the introductory books for learning these languages, they are foundational to the use of the language.

101. As a practical note on the use of concatenation, programmers often embed debug statements in their code. Debug statements usually contain information that is concatenated together. Oftentimes, this is in the form of a timestamp concatenated with a message. The message itself may contain values that are concatenated together to generate the output string. Developers use concatenation heavily when generating debug output or operating on files that

include file paths and file names. Concatenation would be well known to a POSA in this field as of March 6, 2000.

102. The '658 Patent's discussion of concatenation reflects the common knowledge regarding concatenation at the time. The '658 Patent discloses: "The server creates a new password by concatenating a secret passcode that is known to the user with the token." Ex-1001, 2:2-4. Similarly, the '658 Patent discloses: "The new password 158 is preferably generated by concatenating the passcode 154 and the token 156." Ex-1001, 9:31-33. The '658 Patent further provides: "The user concatenates the secret passcode with the received token in order to form a valid password, which the user submits to gain access to the secure system." Ex-1001, 2:8-11. The '658 Patent's example of a passcode is "abcd"—which is a string. Ex-1001, 4:52-59. The disclosed token "1234" is also a string. Ex-1001, 4:55. They are sequences of symbols or characters. The password of "abcd1234" (Ex-1001, 4:56) is an example of concatenation as a POSA would have known and used well before March 6, 2000. When combining two strings (such as the disclosed token and passcode), it is what a POSA would naturally have done.

E. Databases

103. Databases were well-known long before March 6, 2000. As the '658 Patent acknowledges, it was not disclosing any new database technology:

The user database 114 is preferably similar or identical to the database

accessed by the authentication module 112 that stores user ID and password data (or passcode and token data) in operating systems such as Windows NT. In alternative embodiments, the user database 114 can be **any database capable of storing user ID and password data.**

Ex-1001, 5:15-21.

104. Associating a phone number with a user ID and password was also covered in well-known schemas prior to March 6, 2000. For example, the Monkey Technical Overview discloses “user database modules” that “handle the mapping from user names to the corresponding mobile phone numbers by performing a lookup in the user database.”

7. monkey implementation

The monkey authentication server consists of four different kinds of modules which are at runtime instantiated as processes. [top](#)

a. User database modules

These modules handle the mapping from user names to the corresponding mobile phone numbers by performing a lookup in the user database. monkey currently includes user database modules for accessing database management systems via LDAP, SQL and ODBC (Windows NT only), and for highly efficient indexed flat file user databases. Aiming at compatibility, monkey is designed to integrate with an existing database infrastructure, instead of maintaining a separate dedicated database of monkey users. [top](#)

Ex-1002, 97.

105. Directory services like the Lightweight Directory Access Protocol (LDAP) (referenced above in the Monkey Technical Overview) and Microsoft's

Active Directory existed prior to March 6, 2000, and were used to store IDs, addresses, emails, phone numbers, etc.

106. LDAP was developed in 1993 by Tim Howes and his colleagues at the University of Michigan. It was created to be a lightweight, low-overhead version of the X.500 directory services protocols used at the time.

107. Following this milestone, Kurt Zeilenga started the OpenLDAP Project by releasing OpenLDAP 1.0 in 1998. This version included advanced security features, updated platform support, and bug fixes. It was also the first entirely open-source suite of client and server applications derived from LDAPv3.3.

108. RFC2256 from December 1997 is “A Summary of the X.500(96) User Scheme for use with LDAPv3” (Ex-1016). As stated in the document:

This document provides an overview of the attribute types and object classes defined by the ISO and ITU-T committees in the X.500 documents, in particular those intended for use by directory clients. This is the most widely used schema for LDAP/X.500 directories, and many other schema definitions for white pages objects use it as a basis.

Ex-1016, 1.

109. RFC2256 specifically includes storing a phone number:

5.21. telephoneNumber

```
( 2.5.4.20 NAME 'telephoneNumber' EQUALITY telephoneNumberMatch
  SUBSTR telephoneNumberSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.50{32} )
```

Ex-1016, 6.

110. The above description of the state of the art as of March 6, 2000, demonstrates that each of the limitations recited in the Challenged Claims had already been included as features in authentication and computing. This prior art provides motivation for a POSA to modify and combine the prior art identified in the Ground (Sormunen and Perlman) below to establish that the Challenged Claims recited nothing more than a combination of prior art elements, each used for its normal and intended purpose, and thus the recited limitations are an obvious modification of the cited prior art.

VIII. Claim Construction

111. I have been informed that an obviousness analysis requires understanding the scope of the claims.

112. I have been informed that during an *inter partes* review proceeding, the terms of the claims of the '658 Patent should be given their ordinary and customary meaning as understood by a POSA in light of the specification and prosecution history. For the purposes of my analysis, I do not believe that any of the claim terms require a specific construction. However, I address some points below regarding what a POSA would consider the ordinary and customary meaning.

A. Preambles

113. I have been informed that claims start with a “preamble.” I have been informed that the preamble includes what is called a “transitional phrase.” I have

been informed that the transitional phrase “consisting of” restricts the claim to only those recited steps or elements specified in the claim. I have been informed that the transitional phrase “comprising” is open-ended and does not exclude any unrecited steps or elements.

114. Claims 1-7 of the '658 Patent use the transitional phrase “comprising,” thus I understand they are open-ended and do not exclude any unrecited steps or elements.

115. I have been informed that a preamble is generally not considered to limit the claims. However, I have been informed that there are circumstances where a preamble can be limiting. I have been informed that there is no litmus test for when a preamble is limiting, but a preamble can be found to be limiting when it recites essential structure or steps, or if it is necessary to give life, meaning, and vitality to the claim.

116. I do not address whether the preamble of any claims of the '658 Patent are limiting. My analysis below includes alternative or optional analysis that assumes the preambles are limiting.

B. Order of Steps

117. I have been informed that the order in which the steps of a claim are listed in a patent is not necessarily the required order the steps have to be performed. I have been informed that a particular sequence of steps is required when logic or

grammar indicates it is required, or when the specification directly or implicitly requires an order of steps.

118. Claim 1 recites: “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.”

119. Claim 1 also recites: “transmitting the token to the personal communication device.”

120. Claim 5 recites: “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.”

121. Claim 5 also recites: “a communication module configured to transmit the token to the personal communication device through the cell phone network.”

122. It could be assumed that the token becomes known to the user when it is transmitted to the personal communication device. Thus, the password would have to be created prior to transmission of the token to the personal communication device.

123. This is consistent with the specification of the '658 Patent which shows, for example, in FIGs. 2A and 2B that the user is given the token so that he or she

can type it into the user interface. Ex-1001, FIGs. 2A and 2B. For example, the '658 Patent provides: "In the preferred embodiment, the user 108 combines the passcode 154 and the token 156 by concatenation to form the password 158." Ex-1001, 7:42-45; Ex-1001, 9:54-60 ("The user 108 preferably concatenates his memorized secret passcode 154 with the valid token 156 to create the password 158."). The user could not do so if the token did not become known to the user.

124. However, as I explain below, it does not alter my analysis whether the token becomes known to the user or not. The prior art teaches the token being requested by and transmitted to a user over a cellular network via a personal communication device and then automatically provided by the personal communication device to a computer terminal through which the user authenticates to an account on a secure computer network. The prior art also teaches using a mobile device's display to show the token to the user. Thus, for purposes of my analysis, I assume that claims 1 and 5 require that the token is at least not known to the user at the time the password is created. The token may subsequently become known to the user.

C. Passcode, Token, and Password

125. The '658 Patent uses the terms "passcode," "token," and "password." A POSA would understand that each of them are, by their ordinary and customary meaning, a string with different labels according to their function or role. In the sole

example provided in the '658 Patent, it discloses a “memorized passcode of ‘abcd,’ a valid token of ‘1234,’” and forming the password “abcd1234.” Ex-1001, 4:52-56. A “passcode” is a “secret [string] known to the user.” Ex-1001, 2:13-14 (“secret information known to the user, such as the passcode”). It is information that can be associated with a user ID. Ex-1001, 8:53-55 (“[T]he control module 402 associates a user ID with a passcode 154 and phone number of a user’s personal communication device 106.”). A token is a string “that is provided to the user through an object possessed by the user.” Ex-1001, 2:14-15. The password is a string generated based on the token and the passcode, such as by concatenation (no other techniques are discussed). Ex-1001, 2:2-4 (“The server creates a new password by concatenating a secret passcode that is known to the user with the token.”). This is consistent with disclosure regarding concatenation of the token and passcode to create the password. As I discuss above in the state of the art (Section VII.D), it was well-established by March 6, 2000, that concatenation was (and is) a function performed on strings. When combining two strings to generate a new string, a POSA would have viewed concatenation as an obvious or even the most obvious choice for combination due to its foundational nature and simple use.

IX. Claims 1-7 of the '658 Patent are Obvious Over the Sormunen in View of Perlman

126. The international patent application described below (Sormunen) discloses using short messages over a cell phone network for a much faster way of

generating and providing authentication data (e.g., passwords) for new subscribers to an information service. The request and the response are both sent over a separate cell phone network. The user can then use the new authentication data to access the information service, which is on a separate network. Thus, Sormunen discloses what the patent examiner thought was not shown in the prior art when he allowed the '658 Patent to issue.

A. The Sormunen Reference

127. Sormunen (Ex-1004) is an international patent application filed on February 6, 1997, entitled “Method for obtaining at least one item of user authentication data.” Sormunen was published on August 28, 1997, and claims priority to a Finnish patent application filed on February 23, 1996. I have been informed that Sormunen is prior art to the '658 Patent.

128. Sormunen discloses “a method and system for obtaining at least one item of user specific authentication data, such as a password and/or a user name.” Ex-1004, 1:3-5. A POSA would understand that a token could also be one item of user specific authentication data. Sormunen discusses the use of “information services,” which can be connected to via a “data transmission connection” over a “telecommunication network or a mobile communication network,” such as a “wireline telecommunication network.” Ex-1004, 1:8-13, 8:5-8. To use the information service, “user specific authentication data is required, for example a user

name and password.” Ex-1004, 1:14-15. The user name and password “enable the information service provider to control the user using the information service” and “prevent unauthorized use of the information service.” Ex-1004, 1:17-22.

129. Sormunen discloses that “[a] user name is user specific and it is usually not changed in different connection set-ups.” Ex-1004, 1:30-31. Regarding passwords, Sormunen discloses that the use of “[o]ne single password valid as long as the user is a registered subscriber to the service” is “used mainly used in services with less need for security.” Ex-1004, 1:34-36. Sormunen discloses that an alternative is “[a] list of single-connection passwords, each valid for one connection.” Ex-1004, 2:1-2. However, a drawback of this approach is “that the list has to be kept safe and account of the last used password has to be kept in one way or another. Thus the possibility of abuse is great, especially if the list and the user name are preserved in the same place.” Ex-1004, 20-24. Sormunen discloses that another option is “[a] periodical password valid for a predefined period of time.” Ex-1004, 2:13. However, Sormunen further discloses that “regardless of which password type is used, it is the user of the service who is to a great extent responsible for data security, and the service provider has few possibilities to prevent and control abuse for example in case the password falls into the wrong hands.” Ex-1004, 26-29.

130. Fig. 2 of Sormunen “shows a method for transmitting a user name and

passwords according to a preferred embodiment of the invention.” Ex-1004, 5:26-27.

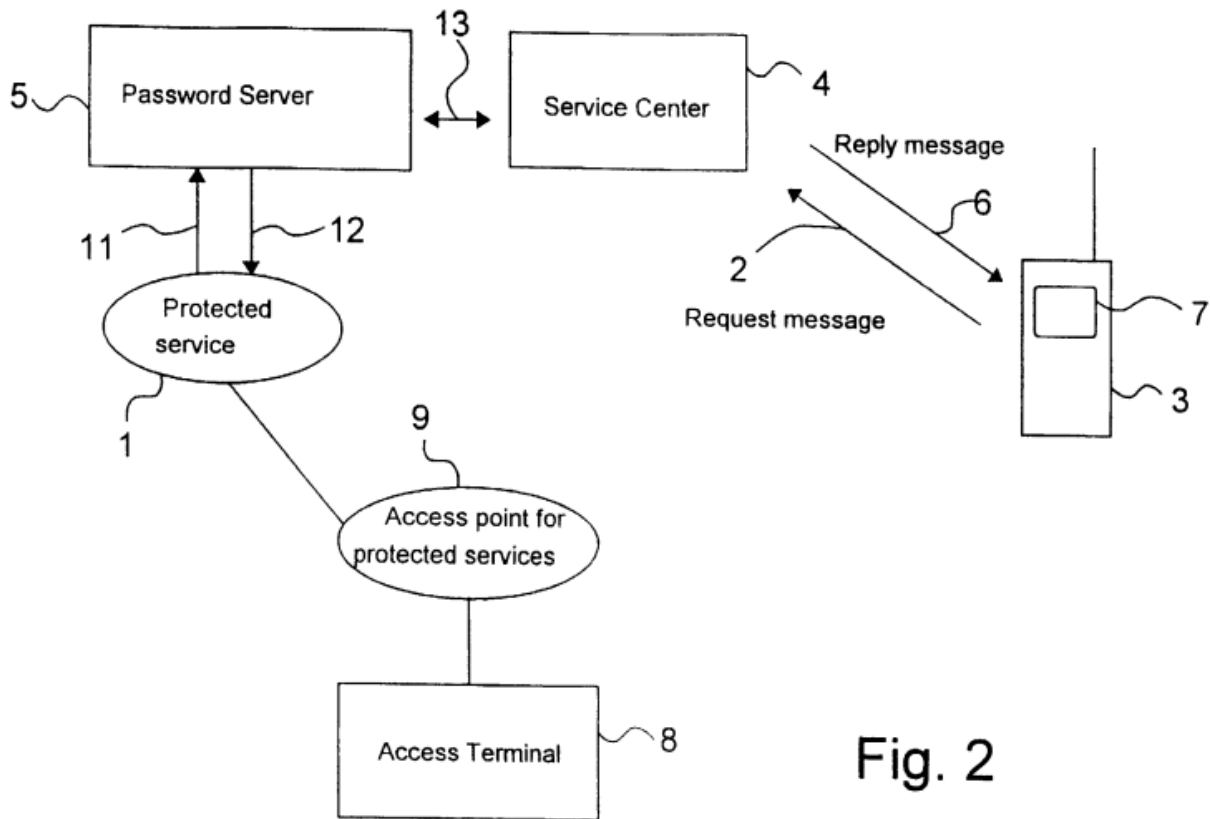


Fig. 2

131. Sormunen discloses that a user may wish to use “protected service 1.” Ex-1004, 7:6-7. To obtain “a password” or “list of passwords” to use protected service 1, “the user of the service sends a short message 2 from the paging terminal 3, such as a mobile station.” Ex-1004, 5:33-38. The mobile station includes “display means 7.” Ex-1004, 7:5-6.

132. Sormunen discloses that “[t]he short message 2 includes a password request and possibly also a subscription request for a new user.” Ex-1004, 5:38-6:2.

The user sends short message 2 to “paging service center 4,” which “is for example in the GSM system advantageously a short message service center.” Ex-1004, 6:32-33; *see also* Ex-1004, 5:6-8 (“It is advantageous to apply the present system in mobile communication systems which include short message service (SMS) or paging.”). The “GSM system” is disclosed as “a mobile communication system in which a cellular network is used.” Ex-1004, 6:1-3. Sormunen provides that “[t]he form of the data depends on the type of the message system used. For example the GSM system allows sending short messages, wherein a GSM mobile station can be used in implementation of the method according to the invention.” Ex-1004, 6:4-7.

133. The paging service center 4 processes the request and “transmits the inquiry to” “password server 5.” Ex-1004, 6:20-23. “The password server 5 processes the message and forms a reply message containing one or more passwords and the user name in case a new user is registered.” Ex-1004, 6:23-24. The password server 5 transmits the password and/or user name to the short message service center 4, which forms according to the data a reply message 6, which is sent to the paging terminal 3 preferably in enciphered form.” Ex-1004, 6:35-38. The reply can be shown to the user, such as by using display means 7. Ex-1004, 7:4-6.

134. The user can then use “Access Terminal” 8 to form “a data transmission connection to the verification service 9 of protected service 1.” Ex-1004, 7:9-10. Access terminal 8 is also disclosed as data processor 8, and can communicate with

the protected service 1 (information service) through “a modem connection to a wireline telecommunication network.” Ex-1004, 8:5-7. The user submits a user name and password through access terminal 8 to verification service 9. Ex-1004, 7:9-13.

135. The verification service 9 transmits the given data to the service 1, which sends a check request 11 of the user name and the password to the password server 5.” Ex-1004, 7:11-14. “The password server 5 examines the data and communicates in a reply message 12 to the service 1 whether the user name and the password are given correctly,” and if they are, the user is given a data transmission connection to the service 1. If they are not correct, the user is prevented from using the service. Ex-1004, 7:14-18.

136. Sormunen further discloses: “[T]he present invention can be applied also for obtaining a personal identity number (PIN) of bank and credit cards and corresponding charge cards. Thus when the charge card is being ordered, the number of the orderer’s paging device or mobile station can be given, wherein the supplier of the charge card transmits the personal identity number connected to the charge card to the paging device or the mobile station of the user.” Ex-1004, 9:26-32. “The method according to the invention can be used for requesting a new personal identity number for a charge card which is already in use, wherein the identity number is transmitted to the paging device or the mobile station of the user.” Ex-1004, 9:34-

37.

137. Sormunen is analogous art to the '658 Patent. Sormunen is from the same field of endeavor as the '658 Patent: user authentication. Even assuming that it was not, it was also reasonably pertinent to at least one issue concerning the inventors of the '658 Patent. For example, the inventors of the '658 Patent were concerned with eliminating the need for an additional device to provide user authentication information by instead providing it using “a device that many users already carry—a personal communication device such as mobile phones or pagers.” Ex-1001, 1:55-60. Sormunen discloses using a paging terminal/mobile station to communicate using short messages over a cellular network to request and receive user authentication information. Thus, Sormunen was reasonably pertinent to at least one problem relevant to the inventors the '658 Patent.

B. The Perlman Reference

138. U.S. Patent No. 6,173,400 to Radia J. Perlman, et al. (“Perlman”), has a filing date of July 31, 1998. Ex-1005. I have been informed that Perlman is prior art to the '658 Patent.

139. Perlman relates to “secure communications, and more particularly, to methods and systems for establishing a shared secret between devices connected over a communication medium using an authentication token to provide user authentication, data encryption, and integrity protection.” Ex-1005, 1:6-11.

140. Perlman discloses that “a user name and password only provides a minimal level of use authentication to access the network” and that “[i]f the password is simple (e.g., the user’s birth date) a hacker can easily determine the user’s password and access the network with this information assuming the user’s name.” Ex-1005, 1:24-29.

141. In light of the aforementioned vulnerabilities, Perlman discloses “using an authentication token to provide adequate user authentication, data encryption, and integrity protection.” Ex-1005, 1:9-11. Perlman discloses that “[m]any users currently rely on authentication tokens to provide an additional level of user authentication based on ‘something you have’ (versus ‘something you know,’ like a password).” Ex-1005, 1:38-40. Perlman discloses that “[t]he authentication token can be a time-synchronized token, challenge response token, or any token configured to implement the authentication techniques described herein.” Ex-1005, 6:1-4.

142. Specifically, Perlman discloses using “an authentication token that generates a character string,” wherein the “character string, for example, is a password based on the time of day encrypted with a secret code or a random number.” Ex-1005, 4:38-64. The “character string is communicated to a local device (*e.g.*, a work station) where it can be modified using a predetermined function to produce a result (*i.e.*, a second character string).” Ex-1005, 4:38-64; Ex-1005, 8:49-62; Ex-1005, 11:8-20. The resultant “second character string” is

communicated to a remote device for authentication. Ex-1005, 4:38-64; Ex-1005, 8:55-9:9; Ex-1005, 11:8-20. As I explain above in the state of the art (Section VII.D), a POSA would have understood that concatenation was a predetermined function for modifying a first character string with another character string to produce a second character string.

143. Further, Perlman proposes concatenating a generated character string (i.e., token) with a PIN (i.e., passcode) to act as the password. Ex-1005, 8:14-9:35.

144. Moreover, Perlman discloses that the workstation is simply a “computer capable of sending data to and receiving data from network 160” and includes a “processor, memory, and input/output devices to facilitate human interaction (not shown).” Ex-1005, 5:5-17. This is consistent with what a POSA would have understood regarding a workstation as of March 6, 2000.

145. Perlman is analogous art to the '658 Patent. Perlman is from the same field of endeavor: user authentication. However, even assuming that Perlman was not from the same field of endeavor, it was reasonably pertinent to at least one issue concerning the inventors of the '658 Patent. The inventors of the '658 Patent were concerned with passwords being secure and not being guessed by hackers. Ex-1001, 1:20-31. Perlman discusses the same concern and discusses approaches for forming more secure passwords from known and generated strings. Ex-1005, 1:24-28. Further, the inventors of the '658 Patent sought to obtain the benefits of using

devices like the SecurID card, just using a mobile phone or pager instead. Ex-1001, 1:56-59. Thus, beneficial uses, techniques, and solutions involving token devices as disclosed by Perlman would therefore be relevant to the inventors of the '658 Patent who sought to obtain the same benefits of using token devices. Ex-1005, 3:12.

C. Motivation to Combine the Teachings of Sormunen and Perlman

146. A POSA would have found it obvious as of March 6, 2000, to combine the teachings of Sormunen with the teachings of Perlman. A POSA would have been motivated to modify Sormunen with the teachings of Perlman to allow for greater security and ease of use.

147. Sormunen concerns generating passwords for new subscribers to an information service. Sormunen discloses that in the prior art, a user wishing to gain access to an information service would send a request for a subscription, be sent a form, fill out the form, and send it back to the service provider. Ex-1004, 2:31-35, 3:12-18. “The information service provider subsequently handles the form and allots the user the user specific authentication data and sends it for instance by mail, electronic mail or facsimile (block 107).” Ex-1004, 3:19-21. After receiving the user specific authentication data, the user can start using the information service. Ex-1004, 3:21-22. The “user specific authentication data” is “for example a user name and password.” Ex-1004, 1:14-15. It can also be a PIN. Ex-1004, 9:26-37.

148. Sormunen “enables very fast subscription” including “transmission of

user information in enciphered electronic form and the receiver can be recognized in order to prevent abuse.” Ex-1004, 5:10-18. Sormunen provides that “[a] further advantage of the fast data transmission is that the validity of passwords can be shortened remarkably and security may thus be improved.” Ex-1004, 5:16-18.

149. Sormunen discloses “[t]he transmission of user specific authentication data to the user is performed by using paging or short message service.” Ex-1004, 9:22-24. Sormunen also discloses generating a new PIN and transmitting it to a user’s paging device or mobile station. Ex-1004, 9:34-37. A POSA would appreciate that this could be a “single-connection” password or PIN, and/or a password or PIN “valid for a predefined period of time.” Ex-1004, 2:1-18.

150. This would also allow greater flexibility in letting users select their own password when registering with the service provider. Ex-1004, 3:31-32 (“Information to be filled in includes e.g. forename, surname, a proposal for user name and password.”). By requiring that this selected or initial password be augmented by a generated PIN to create an account password (one that must be created in order for the account to be accessed) the level of security would be increased according to known methods.

151. Perlman discloses that “a user name and password only provides a minimal level of use authentication to access the network” and that “[i]f the password is simple (e.g., the user’s birth date) a hacker can easily determine the

user's password and access the network with this information assuming the user's name." Ex-1005, 1:25-27. Further, he discloses that "it is desirable to establish a shared secret between parties communicating over a network using an authentication token to provide adequate user authentication, data encryption, and integrity protection" Ex-1005, 1:8-12.

152. Sormunen does not solve the recognized security issue concerning user name and password combinations. Thus, a POSA would have been expressly motivated to combine the teachings of Perlman with the teachings of Sormunen to increase security (i.e., minimize the ability of unauthorized third parties to determine a user's password).

153. Sormunen notes that "the service provider has few possibilities to prevent and control abuse for example in case the password falls into the wrong hands." Ex-1004, 2:26-29. A POSA would have recognized that combining the teachings of Sormunen with the teachings of Perlman would have provided a greater ability to prevent and control abuse. Even if the third party obtained the user's initial or selected password, the third party would have to, at a minimum, also obtain the user's new PIN. A POSA would not see a need to bodily incorporate the authentication token device from Perlman given Sormunen's disclosure of requesting and sending user authentication information via SMS to the paging terminals/mobile stations of users, including the disclosed capability of generating

new PINs in response to requests. Instead, a POSA would appreciate and understand how to use Perlman's disclosure in the context of Sormunen's disclosure.

154. Additionally, as I discuss above regarding the state of the art (Section VII), it was well-known to use a reusable password with a one-time password for two-factor authentication. It was a predictable variation to combine them into one string and use that as a one-time password.

155. Further, combining the teachings of Sormunen with the teachings of Perlman would have involved applying a known technique (concatenation of a generated string to a known string) to achieve predictable results (increased security). It was a known technique to concatenate a generated string with a known/preexisting string (password), and known that it would result in a stronger, more secure password.

156. A POSA would have appreciated that Perlman teaches concatenating a known secret character string with a generated character string provided through a token. A POSA would have appreciated that the resulting character string could be used more securely as a password than the original known secret character string. Thus, a POSA would have been motivated to combine the teachings of Perlman with Sormunen. The original password set for the user (including one proposed by the user) could be augmented by concatenating it with a generated PIN. A POSA would appreciate that, according to the teachings of Perlman, this predetermined function

(concatenation) would be known to the password server. Thus, the password server generates a PIN, and then sets the password as the concatenation of the preexisting or initial password and the PIN, which may be randomized according to techniques known to POSAs. The PIN (user authentication information) would then be transmitted to the user via the user's paging terminal/mobile station.

157. Combining the teachings of Sormunen and Perlman was within the skill of a POSA. The modification would have operated in a predictable manner consistent with the state of the art. The communication arrangement of Sormunen was well-known to POSAs, as was password and token generation as described by Perlman (as I discuss in the State of the Art above). Further, Perlman discloses that “authentication techniques consistent with the present invention may be used on” the Internet as well as “other WANs as well as local area networks (LANs), network protocols, and other communication media.” Ex-1005, 5:34-45. Thus, a POSA would have had a reasonable expectation of success in modifying Sormunen with the teachings of Perlman to achieve what is claimed in the '658 Patent and would have needed only routine skill to do so.

D. Detailed Application of Sormunen and Perlman

1. Claim 1

- 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:***

158. If the preamble is limiting, Sormunen discloses a new or preexisting user wishing to gain access to protected service 1 (*first secure computer network*), which requires a user name particular to that user (*the user having a user account on said first secure computer network*). Ex-1004, Fig. 2, 5:33-6:2. As shown in and described with respect to Fig. 2, a user can use an access terminal/data processor to connect to the protected service (electronic information service) through “a modem connection to a wireline telecommunication network.” Ex-1004, 8:5-7. The “first secure computer network” is highlighted in orange in Fig. 2 below.

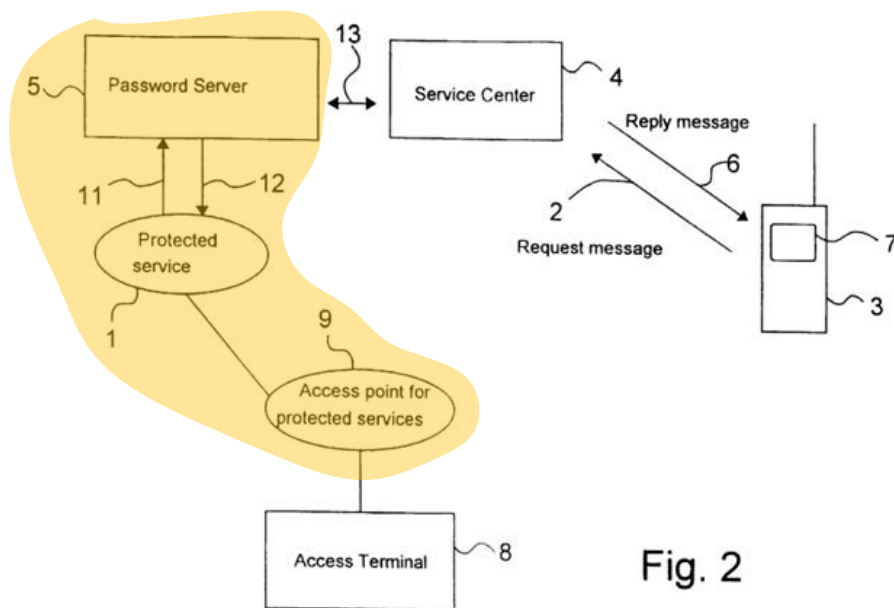


Fig. 2

- ii. ***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;***

159. As discussed above, Sormunen discloses a user wishing to gain access to a protected service (*first secure computer network*). Ex-1004, Fig. 2, 5:33-6:2.

160. Sormunen discloses the use of a “paging terminal” or “mobile station” by a user (*personal communication device*). Ex-1004, 5:35-6:7.

161. Sormunen discloses “[w]hen a new user starts using the information service, the user has to register to the information service provider. This may be done for example by a written subscription request, in which the user gives his or her personal data and other information required, most often by mail, electronic mail (e-mail) or facsimile. In due course, the new user is sent a user name and a password or a list of passwords.” Ex-1004, 2:31-38. Sormunen further discloses that this registration can be done via forms displayed on the “data processor,” with “[i]nformation to be filled in include e.g. forename, surname, a proposal for user and password.” Ex-1004, 2:31-32. Sormunen discloses that the information service provider “forms a record or the like for the user, in which the data of the new user is saved.” Ex-1004, 2:32-36. A POSA would have understood that this user record would have included the user’s cell phone number and would have been stored in a database. A POSA would have understood that a response to the user record request

would require that a return message to be sent to the associated paging terminal/mobile station. The nature of these responses (pager/SMS) would be directed to a phone number. Thus, a POSA would have understood that this user record would have included the user's cell phone number and that this number would have been stored in a database.

162. Further, Sormunen discloses: "The using of the service may be initiated almost immediately after a subscription request has been sent, because transmission of user information is conducted in enciphered, electronic form and the receiver can be recognized in order to prevent abuse." Ex-1004, 5:11-16. Thus, a POSA would have understood that recognizing the receiver for reply message 6 would have inherently required associating the paging terminal/mobile station with the user. Thus, Sormunen discloses that "associating a user with a personal communication device possessed by the user."

163. Sormunen further discloses the use of "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 phone number." Ex-1004, 4:30-34. Sormunen discloses that "[a] cellular system, such as the GSM system, is a mobile communication system in which a cellular network is used" (*said personal communication device in communication over a second network, wherein said second network is a cell phone network*). Ex-1004, 5:1-3. As disclosed by

Sormunen, the cellular network is different from the first secure computer network. The mobile station communicates over a cellular network (e.g., GSM) with the paging service provider 4 (or short message service center). Ex-1004, 5:38-6:20; Ex-1004, 8:19-22 (“Transmission of short messages between the paging terminal 3 and the short message service center 4 is made preferably at least in part in a wireless manner, for example, by using a mobile communication network.”). Access terminal (or data processor) 8 can communicate with protected service 1 over “a modem connection to a wireline telecommunication network.” Ex-1004, 8:5-7. Thus, the cellular network is different than the wireline telecommunication network disclosed by Sormunen used to gain access to the protected service. This specifically addresses the examiner’s reason for allowance. Ex-1002, 294-295.

164. As highlighted in green below, Sormunen discloses the paging terminal/mobile terminal in communication over a cell phone network that is different than the first secure computer network (orange).

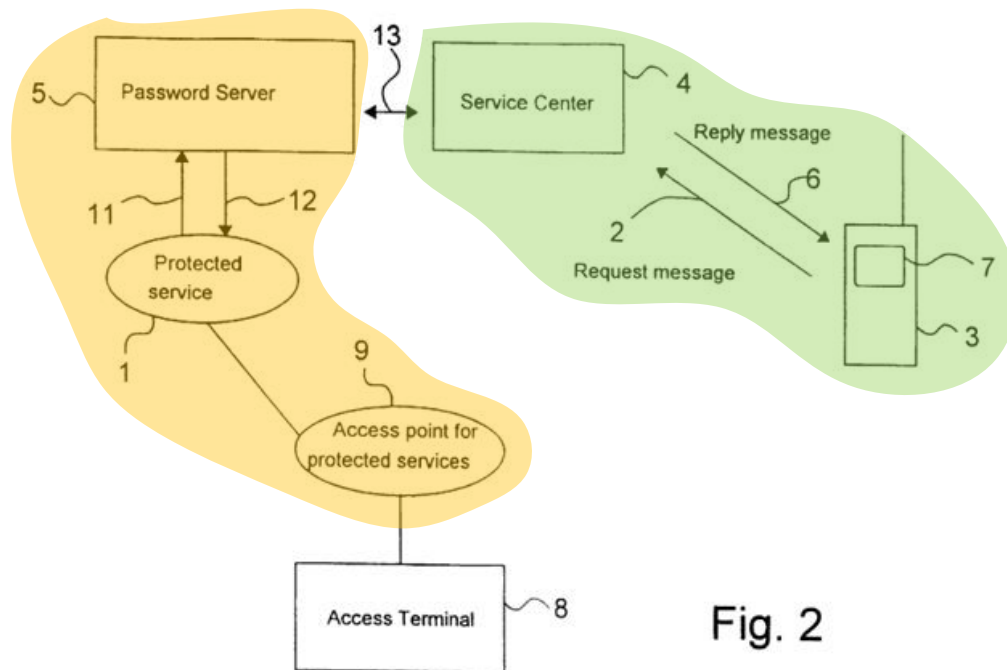


Fig. 2

- iii. ***receiving a request from the user for a token via the personal communication device, over the second network;***

165. Sormunen in view of Perlman teaches “receiving a request from the user for a token via the personal communication device, over the second network.”

166. Sormunen discloses “receiving a request from the user for a token via the personal communication device over the second network.” As underlined below in annotated Fig. 2 of Sormunen, Sormunen discloses receiving request message 2 (*receiving a request from the user*) via a paging terminal/mobile terminal (*personal communication device*) over the cell phone network (*second network*).

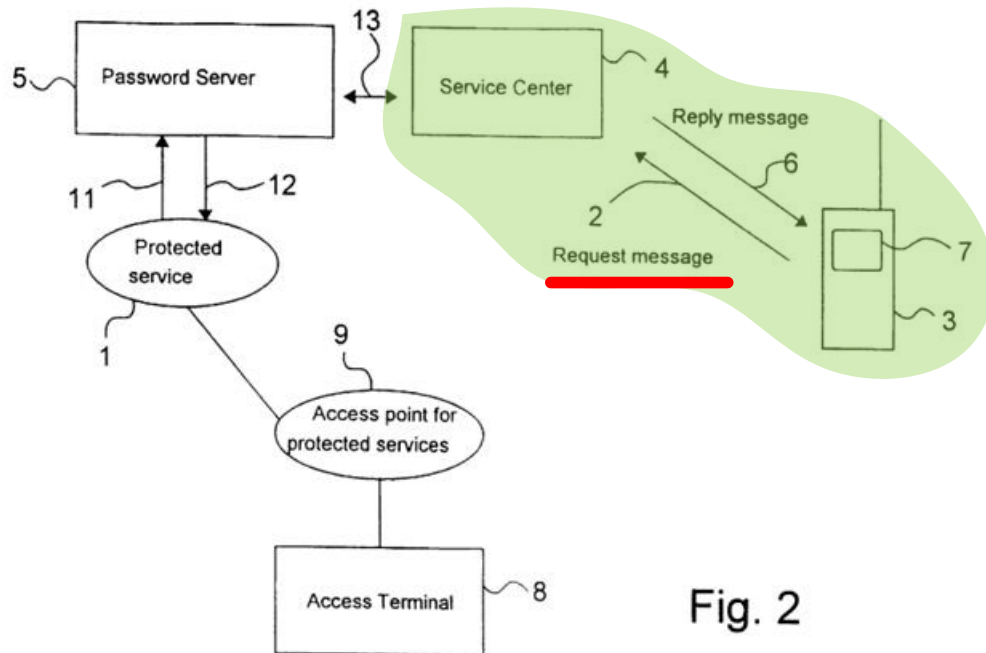


Fig. 2

167. Sormunen discloses: “The short message 2 includes a password request and possibly also a subscription request for a new user.” Ex-1004, 5:38-6:2. A POSA would understand that upon account creation, a password (string) could be provided to the user. A POSA would understand that this password would have the same role or function as the claimed “passcode.”

168. Sormunen also discloses requesting and receiving a new PIN via a personal communication device. Ex-1004, 9:26-37. A POSA would have understood that a PIN is also one user specific authentication data disclosed in Sormunen, and that Sormunen discloses requesting and receiving them over a cell phone network. Ex-1004, 9:26-37. Further, as reflected in the state of the art, a POSA would appreciate that a password and a PIN could be used together for greater

security. For example, they could be used together to address the known problem of a third party obtaining (e.g., guessing, intercepting) one item of user specific authentication data. A POSA would have found it obvious for the new password to be combination of the known password (*passcode*) and the PIN (*token*) generated in response to the request.

169. Further, Perlman teaches using a character string generated by an authentication token to augment an existing character string. Ex-1005, 4:38-64; Ex-1005, 8:49-9:9; Ex-1005, 11:8-20. Thus, a POSA would have appreciated that Perlman teaches augmenting a known character string using a requested character string unknown to the user, at least at that point (*token*).

170. The '658 Patent does not use the term “cell phone network” outside of the claims. However, a “communication module 118” is disclosed which utilizes a “a text messaging service provider 104, which may be a pager or mobile phone service provider.” Ex-1001, 5:32-40. Thus, a “second network” as recited in this claim element includes a broad range of mobile phone capabilities and communications that are similarly disclosed in Sormunen. For example, the '658 Patent discloses that the personal communication device “is preferably a pager or mobile phone having SMS (short message service) receive capability. SMS is a secure text messaging capability that is incorporated into most digital mobile phones.” Ex-1001, 4:8-10. Sormunen discloses the use of SMS. Ex-1004, 5:6-8

(“It is advantageous to apply the present system in mobile communication systems which include short message service (SMS) or paging.”).

- iv. *generating a new password for said first secure computer network based at least upon the token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user;***

171. Sormunen in view of Perlman teaches “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.”

172. Sormunen discloses: “The short message 2 includes a password request and possibly also a subscription request for a new user.” Ex-1004, 5:38-6:2. Sormunen also discloses that this request could be for a new PIN. Ex-1004, 9:34-37.

173. Sormunen discloses that upon account setup, the new user may have a password assigned or selected. Ex-1004, 3:25-32. A POSA would have understood that this initial password teaches the claimed “passcode.” A POSA would have appreciated that it is a string known to the user and known to the system. However, as explained above, a POSA would understand that security can be improved by augmenting it with a PIN to create a more secure password. Thus, a POSA would know from Sormunen to combine the disclosed initial password with the new PIN

to create a new password. A POSA would understand that a PIN would commonly be generated by known techniques to produce a randomized string.

174. Perlman discloses generating a character string and “communicat[ing] it to a local device (*e.g.*, a work station) where it can be modified using a predetermined function to produce a result (*i.e.*, a second character string).” Ex-1005, 4:38-64; Ex-1005, 8:49-9:9; Ex-1005, 11:8-20. The resultant “second character string” is communicated to a remote device for authentication. Ex-1005, 4:38-64; Ex-1005, 8:49-9:9; Ex-1005, 11:8-20. A POSA would have understood that concatenation is a predetermined function for modifying a first character string with another character string to produce a second character string.

175. A POSA would have appreciated that Perlman teaches concatenating a known secret character string with a generated character string provided through a token. A POSA would have appreciated that the resulting character string could be used more securely as a password than the original known secret character string. Thus, a POSA would have been motivated to combine the teachings of Perlman with Sormunen. The original password set for the user (including one proposed by the user) could be augmented by concatenating it with a generated PIN. A POSA would appreciate that, according to the teachings of Perlman, this predetermined function (concatenation) would be known to the password server. Thus, the password server generates a PIN, and then sets the password as the concatenation of the preexisting

or initial password and the PIN, which may be randomized according to techniques known to POSAs. The PIN (user authentication information) would then be transmitted to the user via the user's paging terminal/mobile station.

176. Sormunen and Perlman also disclose that the token is "not known to the user." At the time it is generated in response to the request, it is inherently not known to the user. After it is transmitted to the user's paging terminal/mobile station 3, Sormunen discloses that it can become known to the user by showing it on display means 7. Ex-1004, 7:4-6 ("The reply message 6 arrived to the paging terminal 3 can be shown to the user for example by display means 7 of a mobile station used as a paging terminal."). However, Sormunen also discloses that a "data processor," such as access terminal 8, can be "coupled to a mobile station." Ex-1004, 6:11-12. Perlman similarly discloses that "the workstation can read the character string automatically from the authentication token after the user has entered a PIN into the workstation." Ex-1005, 8:60-62. Thus, a POSA would understand that Sormunen and Perlman disclose that a token may not be not known the user even after the new password is created because it can be read automatically by the access terminal from a coupled mobile station.

v. *setting a password associated with the user to be the new password;*

177. Sormunen and Perlman teach "setting a password associated with the user to be the new password." The password server of Sormunen is disclosed as

setting passwords associated with users. Ex-1004, 5:38-6:2, 6:22-30. A POSA would appreciate that the password server would set the password associated with the user as the preexisting password augmented by the generated PIN according to a predetermined function, as taught by Perlman. Ex-1005, 4:38-64; Ex-1005, 8:49-9:9; Ex-1005, 11:8-20.

vi. *activating access the user account on the first secure computer network;*

178. Sormunen disclose this step. Sormunen discloses: “The short message 2 includes a password request and possibly also a subscription request for a new user.” Ex-1004, 5:38-6:2. Sormunen further discloses: “The using of the service may be initiated almost immediately after a subscription request has been sent, because transmission of user information is conducted in enciphered, electronic form and the receiver can be recognized in order to prevent abuse.” Ex-1004, 5:11-16. The user has an account with the protected service 1.

vii. *transmitting the token to the personal communication device;*

179. Sormunen teaches “transmitting the token to the personal communication device.” Sormunen discloses: “The password server 5 transmits the password and/or the user name to the short message service center 4, which forms according to the data a reply message 6, which is sent to the paging terminal 3 preferably in enciphered form.” Ex-1004, 6:35-38. Reply message 6 is underlined

in red in annotated Fig. 2 of Sormunen below.

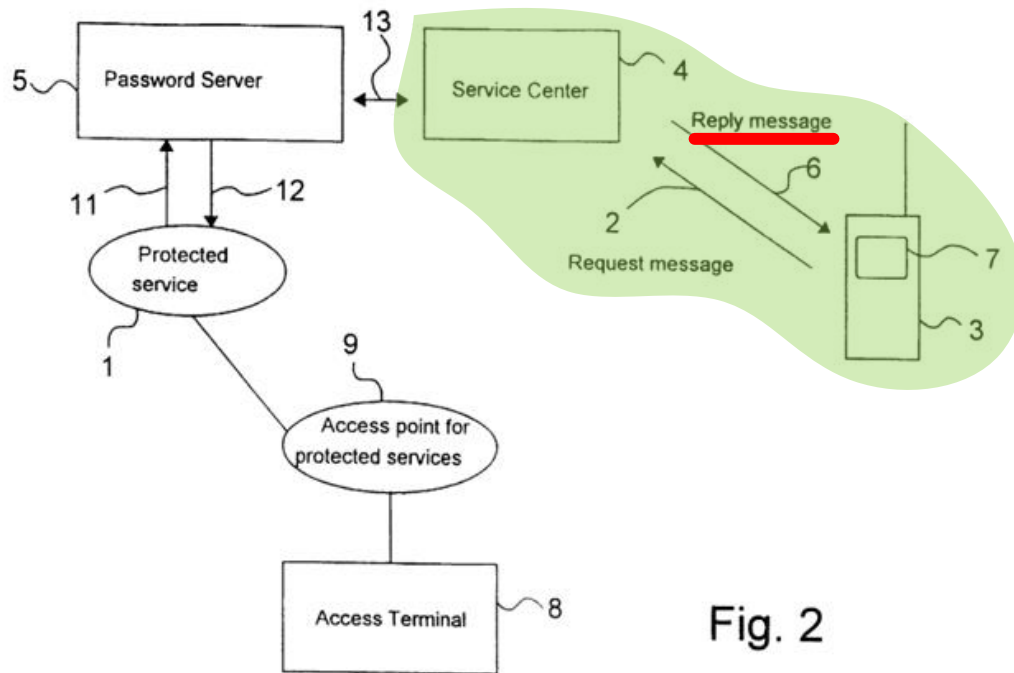


Fig. 2

viii. receiving the password from the user via the first secure computer network; and

180. The combination of Sormunen and Perlman discloses “receiving the password from the user via the first secure computer network.” As shown in annotated Fig. 2 of Sormunen below, Sormunen discloses receiving the password from the user via the first secure computer network (orange).

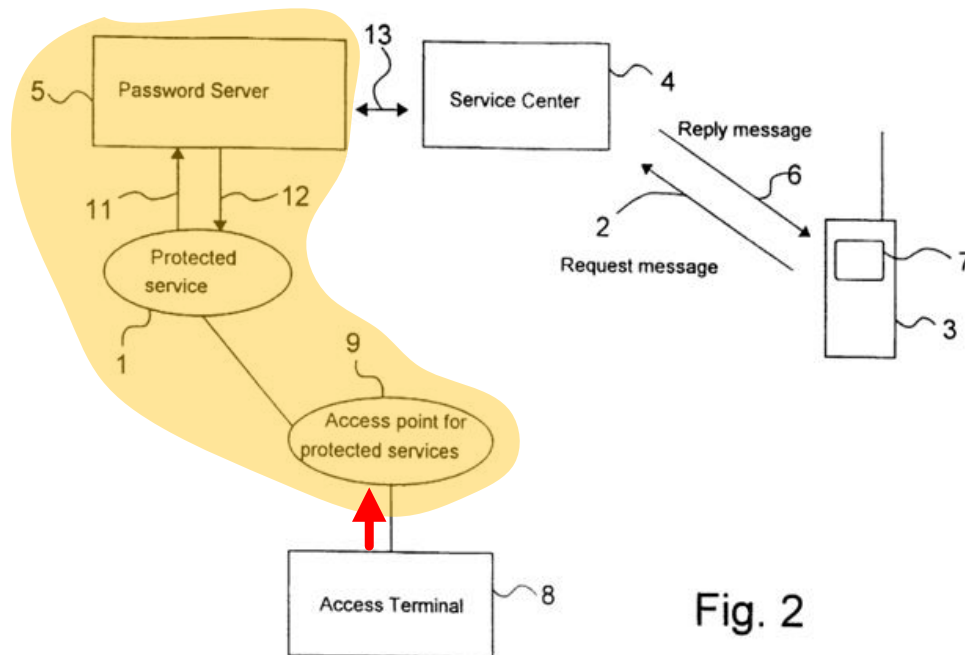


Fig. 2

- ix. ***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.***

181. Sormunen in view of Perlman teaches 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.

182. Sormunen discloses that when the password submitted through access terminal 8 matches the one in the system, the user is given access (*access to the account in response to the password*). Ex-1004, 7:9-20 (“After the user has given his or her user name and the valid password, the verification service 9 transmits the

given data to the service 1, which sends a check request 11 of the user name and the password to password server 5. The password server 5 examines the data and communicates in a reply message 12 whether the user name and the password are given correctly. If the data is correct, the user has a data transmission connection from the data processor 8 to the service 1.”). Further, Sormunen discloses that passwords are only valid for a predetermined amount of time, so access will be denied if not received within that period (*deactivates the account within a predetermined amount of time after activating the account, such that said account is not accessible through any password via the secure computer network*). Ex-1004, 2:13 (“[A] periodical password valid for a predefined period of time.”); Ex-1004, 5:16-18 (“A further advantage of the fast data transmission is that the validity of passwords can be shortened remarkably and security may thus be improved”). Thus, even if the password is correct, the user would not be able to gain access if the validity period has ended (*said user account is not accessible through any password, via said first secure computer network*).

2. Claim 2

The method of claim 1, wherein the new password is generated by concatenating the token and the passcode.

183. Claim 2 is obvious over Sormunen in view of Perlman. Claim 2 provides that the password generated by claim 1 is generated by “concatenating the token and the passcode.” Combining the initial/preexisting password (passcode) and

generated PIN (token) by concatenating them would have been obvious to a POSA. It would have been common sense to combine them by concatenation.

184. Even if it was not common sense, Perlman teaches concatenating a string generated by a token with a preexisting secret string to produce a more secure password.

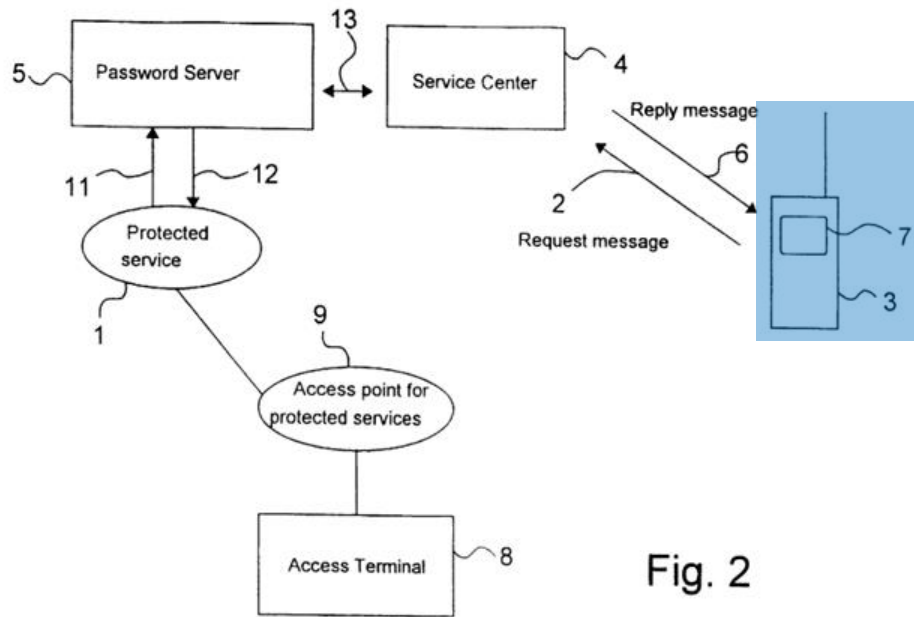
185. As I discuss in the State of the Art section above (Section VI.D), concatenation was taught as part of undergraduate courses (including my own) and was in widespread use as of March 6, 2000. It was also simple for a POSA to use it.

186. Thus, when generating a password as disclosed by the teachings of Sormunen and Perlman, it would have been common sense for a POSA to generate the password by concatenating the passcode and token.

3. Claim 3

The method of claim 1, wherein the personal communication device is a mobile phone.

187. Sormunen discloses “wherein the personal communication device is a mobile phone.” Sormunen discloses a paging terminal (paging terminal 3 in Fig. 2), which may be a “mobile station.” Ex-1004, 5:33-38 (“the user of the service sends a short message 2 from the paging terminal 3, such as a mobile station.”) This is highlighted in blue in Fig. 2 of Sormunen below.



188. The mobile station may communicate via SMS over a cellular network. Ex-1004, 5:38-6:20. Thus, Sormunen discloses “the personal communication device is a mobile phone.”

4. Claim 4

The method of claim 1, wherein the personal communication device is a pager.

189. Sormunen discloses “wherein the personal communication device is a pager.” Sormunen discloses “paging terminal 3,” which may be, “for example a paging device or the like . . . whereby the method of transmitting the reply message to the paging device depends for example on the paging system used.” Ex-1004, 8:33-35. Further, paging service center 4 is also disclosed as being “for example, a paging network controller or a wireless messaging switch.” Ex-1004, 8:36-37.

Thus, Sormunen discloses “the personal communication device is a pager.”

5. Claim 5

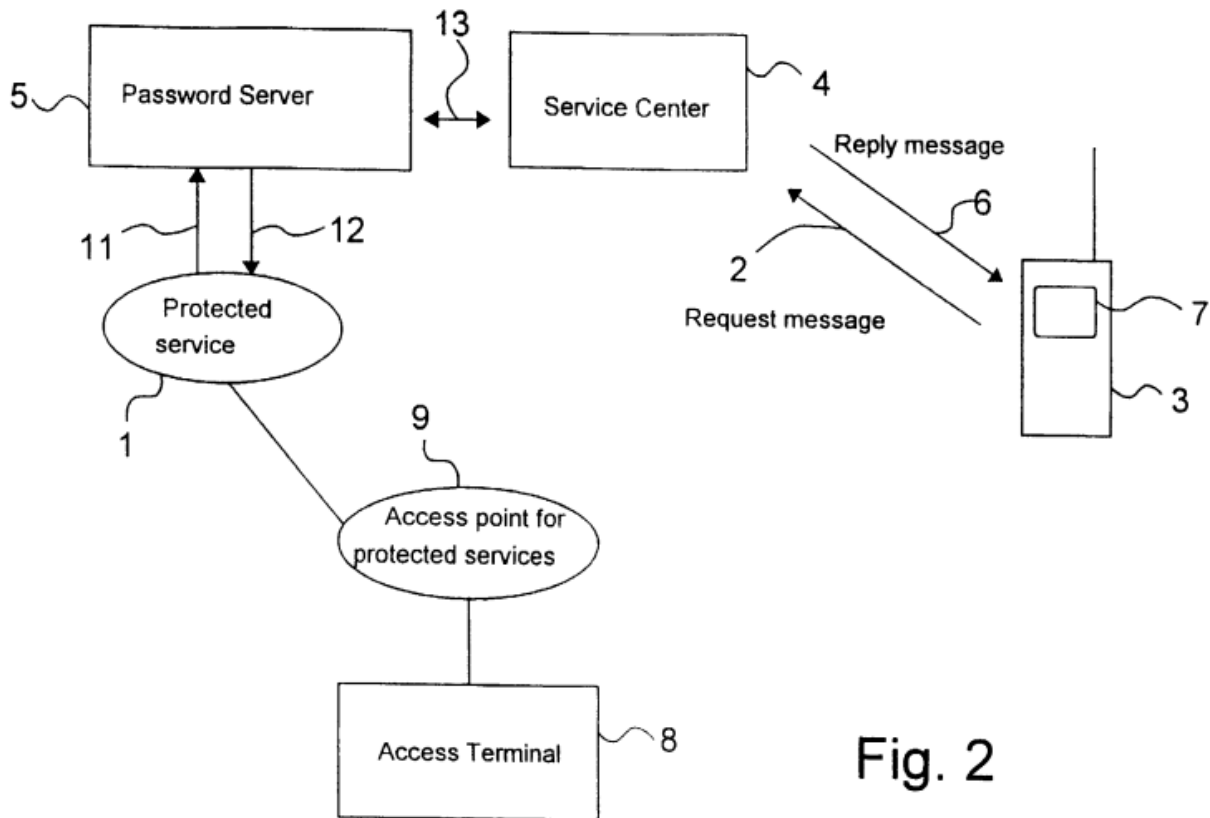
190. Claims 5-7 overlap with claim 1. Claims 5-7 generally describe in functional terms what is listed a step of the method of claim 1. Thus, much of my analysis for claim 1 is applicable to claims 5-7, which I reference back to and incorporate below.

i. A user authentication system comprising:

191. If the preamble is limiting, it is disclosed by Sormunen. Sormunen discloses “a method and system for obtaining at least one item of user specific authentication data, such as a password and/or a user name.” Ex-1004, 1:3-5. Sormunen discusses the use of “information services,” which can be connected to via a “data transmission connection” over a “telecommunication network or a mobile communication network,” such as a “wireline telecommunication network.” Ex-1004, 1:8-13, 8:5-8. To use the information service, “usually user specific authentication data is required, for example a user name and password.” Ex-1004, 1:14-15. The user name and password “enable the information service provider to control the user using the information service” and “prevent unauthorized use of the information service.” Ex-1004, 1:17-22.

192. Fig. 2 of Sormunen “shows a method for transmitting a user name and passwords according to a preferred embodiment of the invention.” Ex-1004, 5:26-

27.



193. Thus, Sormunen discloses a “user authentication system.”

ii. a computer processor;

194. Sormunen teaches “a computer processor.” A POSA would understand that the password server of Sormunen necessarily includes a computer processor. For example, Sormunen discloses: “The service block 1, the password server block 5 and the verification service block 9 shown in the block diagram of Fig. 2, can be placed for example in the mainframe of the service provider or the like, or they can be separate data processors between which data transmission connections are formed.” Ex-1004, 8:9-13. A POSA would understand that the password server

would not function in the way disclosed by Sormunen (or at all) without a computer processor.

- iii. 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;**

195. Please see my discussion above regarding claim 1(ii) (Section IX.D.1.ii). This element is taught by Sormunen. A POSA would have understood that Sormunen utilizes 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.”

196. Sormunen discloses “[w]hen a new user starts using the information service, the user has to register to the information service provider. This may be done for example by a written subscription request, in which the user gives his or her personal data and other information required, most often by mail, electronic mail (e-mail) or facsimile. In due course, the new user is sent a user name and a password or a list of passwords.” Ex-1004, 2:31-38. Sormunen further discloses that this can be done via forms displayed on the “data processor,” with “[i]nformation to be filled in include e.g. forename, surname, a proposal for user and password.” Ex-1004, 2:31-32. Sormunen discloses that the information service provider “forms a record

or the like for the user, in which the data of the new user is saved.” Ex-1004, 2:32-36. A POSA would have understood that this user record would have included the user’s cell phone number, and that such electronic records would be stored in a database. A POSA would have understood that a response to the user record request would require a that return message to be sent to the associated paging terminal/mobile station. The nature of these responses (pager/SMS) would be directed to a phone number. Thus, a POSA would have understood that this user record would have included the user's cell phone number and that this number would have been stored in a database.

197. Further, Sormunen discloses: “The using of the service may be initiated almost immediately after a subscription request has been sent, because transmission of user information is conducted in enciphered, electronic form and the receiver can be recognized in order to prevent abuse.” Ex-1004, 5:11-16. Thus, a POSA would have understood that recognizing the receiver for reply message 6 would have inherently required associating the paging terminal/mobile station with the user. Thus, Sormunen discloses that “user database configured to associate a user with a personal communication device possessed by the user.”

198. Sormunen further discloses “said personal communication device configured to communicate over a cell phone network with the user authentication system.”

- iv. 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;***

199. Please see my discussion above with respect to claim 1(iv) and 1(v) (Sections IX.D.1.iv and IX.D.1.v). This element is taught by Sormunen in view of Perlman. As mentioned above with respect to the “computer processor” element, Sormunen discloses a “password server.” A POSA would know that the password server would necessarily have a computer processor and execute its claimed functions on it. Ex-1004, 8:9-13 (“The service block 1, the password server block 5 and the verification service block 9 shown in the block diagram of Fig. 2, can be placed for example in the mainframe of the service provider or the like, or they can be separate data processors between which data transmission connections are formed.”).

200. Perlman, for example, discloses that “the workstation can read the character string automatically from the authentication token after the user has entered a PIN into the workstation.” Ex-1005, 8:60-62. Similarly, Sormunen discloses that a “data processor,” such as access terminal 8, can be “coupled to a mobile station.” Ex-1004, 6:11-12. Thus, a POSA would understand that Sormunen and Perlman disclose that a token would not be not known the user at the time of

creation of the password and could even not be known to the user after the token is transmitted to the user.

- v. ***a communication module configured to transmit the token to the personal communication device through the cell phone network; and***

201. Please see my discussion above regarding claim 1(vii) (Section IX.D.1.vii). Sormunen in view of Perlman teaches “transmitting the token to the personal communication device.” As shown underlined in red in Fig. 2 Sormunen below, Sormunen discloses “reply message 6.”

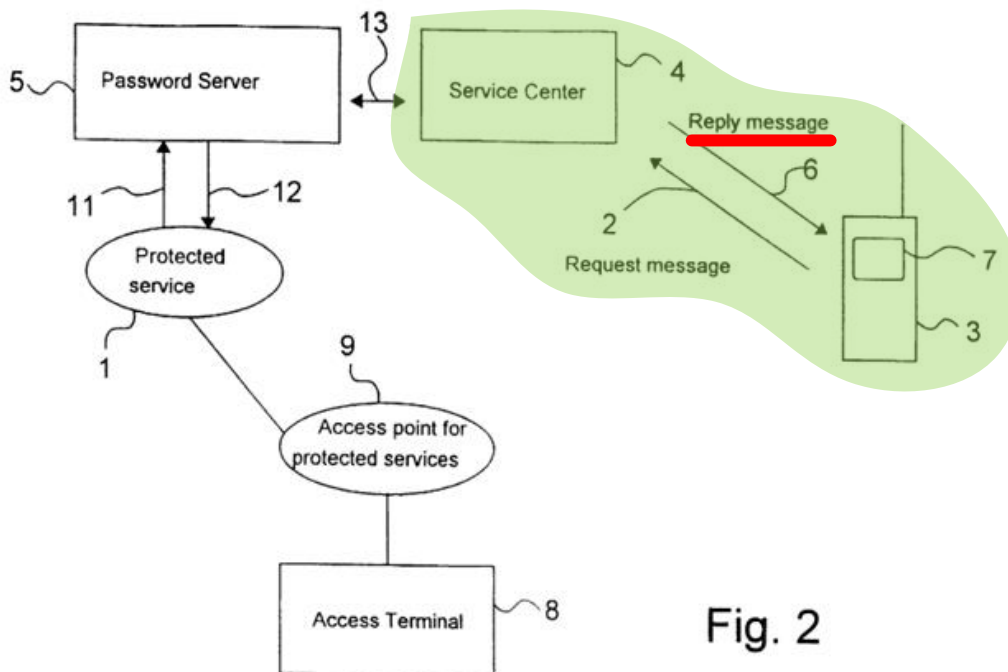


Fig. 2

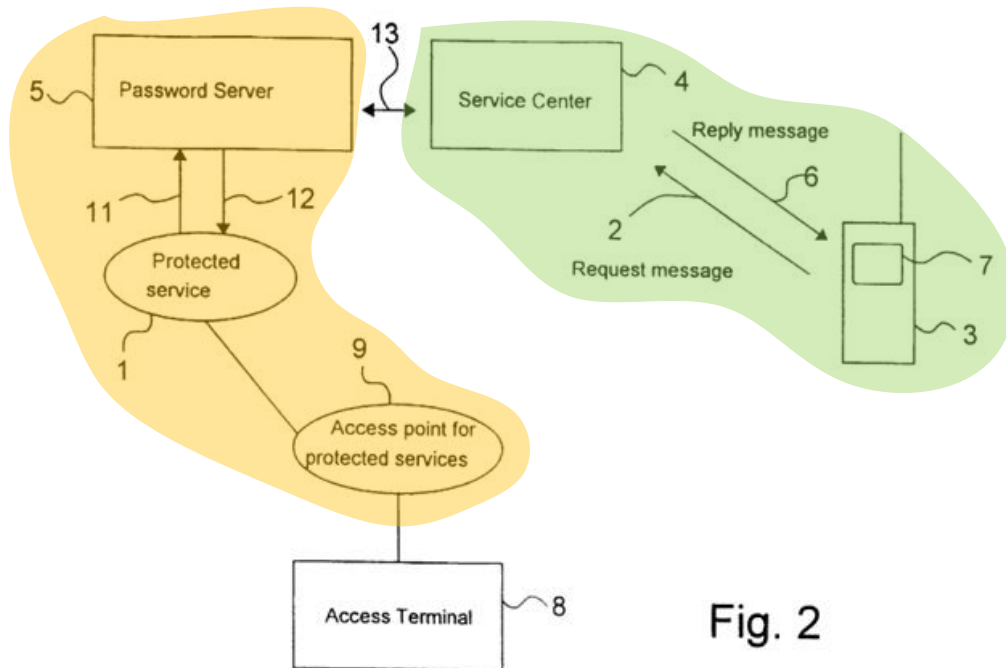
202. Sormunen discloses sending user authentication data through the cell phone network in the reply message: “The password server 5 transmits the password and/or the user name to the short message service center 4, which forms according to the data a reply message 6, which is sent to the paging terminal 3 preferably in

enciphered form.” Ex-1004, 6:35-38.

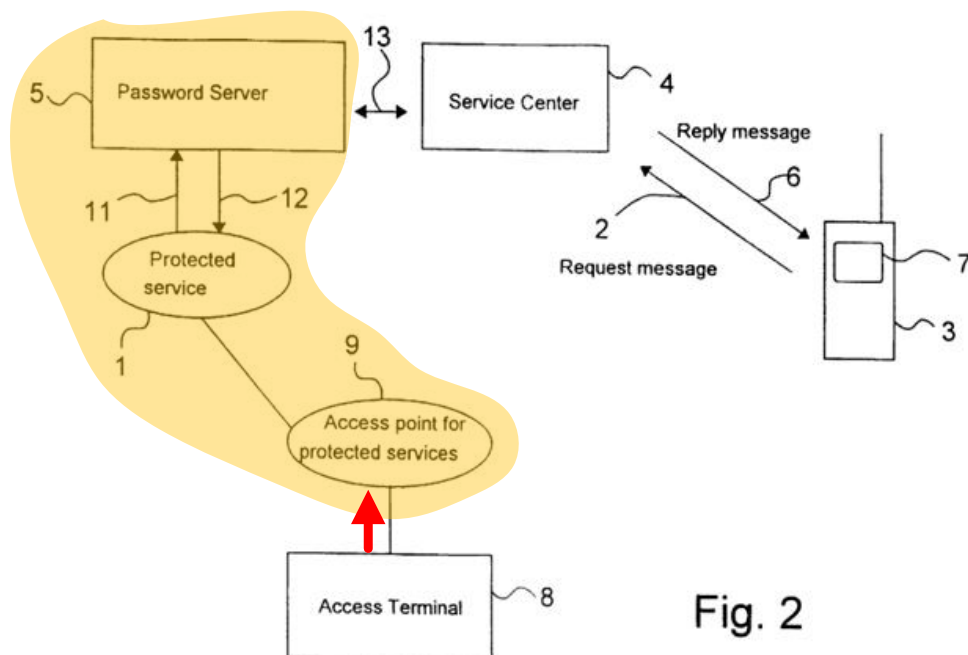
- vi. ***an authentication module configured to receive the password from the user through a secure computer network, said secure computer network being different from the cell phone network, wherein the user has an account on the secure computer network, wherein the authentication module activates access 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.***

203. This element is taught by Sormunen and Perlman as discussed with respect to claim 1(i), (ii), (vi), (viii), and (ix) (Sections IX.D.1.i, IX.D.1.ii, IX.D.1.vi, IX.D.1.vii, and IX.D.1.ix).

204. As shown below in the highlighted Fig. 2 of Sormunen, Sormunen discloses the paging terminal/mobile station in communication over a cell phone network (green) that is different than the first secure computer network (orange) (*a secure computer network, said secure computer network being different from the cell phone network*). The user has an account with the protected service 1 (*wherein the user has an account on the secure computer network*). Ex-1004, 3:25-3:38.



205. As shown below with the red arrow in annotated Fig. 2, Sormunen discloses receiving the password from the user through the secure computer network.



206. When the password submitted through access terminal 8 matches the

one in the system, the user is given access (*access to the account in response to the password*). Ex-1004, 7:9-20 (“After the user has given his or her user name and the valid password, the verification service 9 transmits the given data to the service 1, which sends a check request 11 of the user name and the password to password server 5. The password server 5 examines the data and communicates in a reply message 12 whether the user name and the password are given correctly. If the data is correct, the user has a data transmission connection from the data processor 8 to the service 1.”). Further, Sormunen discloses that passwords are only valid for a predetermined amount of time, so access will be denied if not received within that period (*deactivates the account within a predetermined amount of time after activating the account, such that said account is not accessible through any password via the secure computer network*). Ex-1004, 2:13 (“[A] periodical password valid for a predefined period of time.”); Ex-1004, 5:16-18 (“A further advantage of the fast data transmission is that the validity of passwords can be shortened remarkably and security may thus be improved”).

6. Claim 6

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

207. Please see my discussion above regarding claim 1(iii), 1(iv), and 1(v)

regarding this limitation (Sections IX.D.1.iii-v). This limitation is taught by Sormunen in view of Perlman. As depicted in Fig. 2, service center 4 (which may be a short message service center) is configured to receive request message 2 from paging terminal 3 (mobile station). Ex-1004, 8:19-22 (“Transmission of short messages between the paging terminal 3 and the short message service center 4 is made preferably at least in part in a wireless manner, for example, by using a mobile communication network.”). The disclosure concerning paging service center 4 teaches the claimed function of the “communication module,” and password server 5 teaches the claimed function of the “control module.”

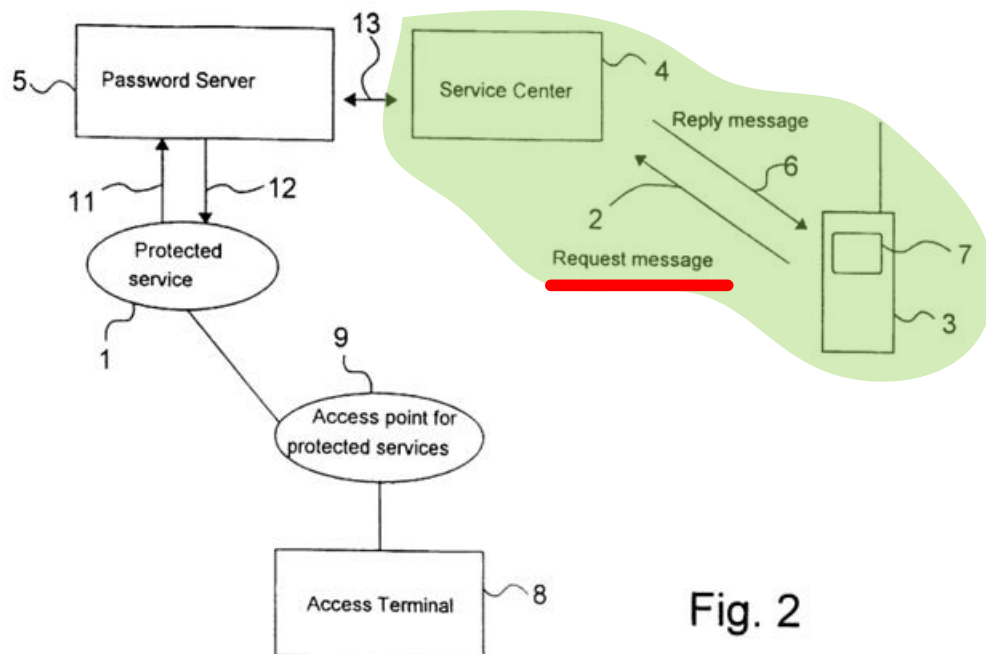


Fig. 2

208. As shown in Fig. 2, password server 5 communicates with paging service center 4 over data transmission connection 13. Ex-1004, 8:15-19 (“The data transmission connection 13 between the short message service center 4 and the

password server 5 can be for example a direct connection by using ISDN/LAN . . . or a corresponding connection. Also this is prior art known as such.”). Sormunen discloses that in response to receiving the request, the password server creates a new password.

7. Claim 7

The system of claim 6, wherein the request is transmitted by the user through the personal communication device.

209. Please see my above discussion regarding claim 1(iii) (Section IX.A.D.1.iii). Sormunen teaches “the request is transmitted by the user through the personal communication device.” As underlined in annotated Fig. 2 of Sormunen below, Sormunen discloses request 2 transmitted by the user via paging terminal 3/mobile station (*personal communication device*).

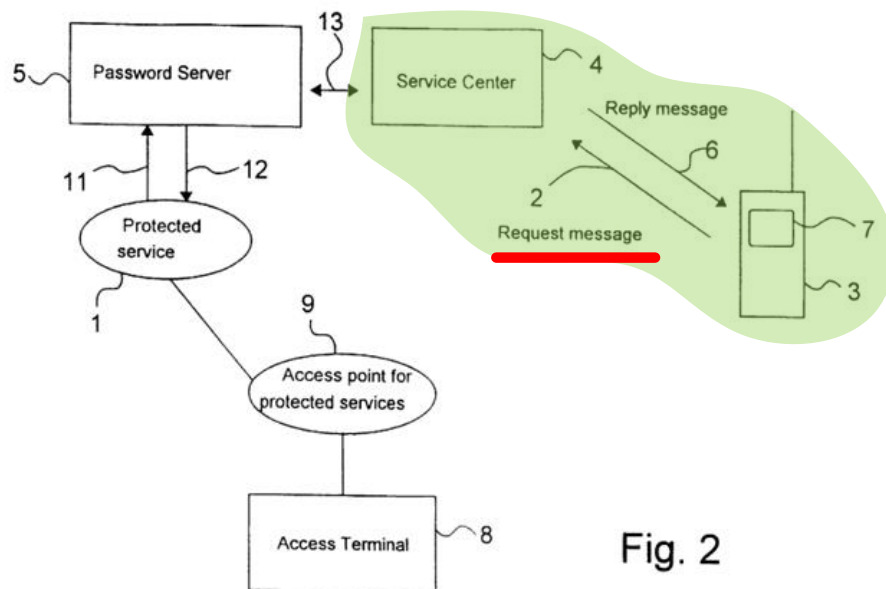


Fig. 2

X. Summary of My Opinions

210. In my opinion, claims 1-7 of the '658 Patent are unpatentable because they would have been obvious based on my review of the '658 Patent, the prosecution history of the '658 Patent, the scope of claims 1-7, the scope and content of the prior art discussed in the Petition, background materials I discuss herein, and the level of ordinary skill in the field of user authentication as of March 6, 2000.

XI. Declaration

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

Date: 9/27/2023

By: Stephen Perkins
Stephen Perkins, Ph.D.

APPENDIX A

STEPHEN PERKINS

☎ (469) 667-1887 | 📍 Houston/Dallas, TX | ✉ perkins@stephen-perkins.com | 🔗 [Linkedin.com/in/perkinsstephenj](https://www.linkedin.com/in/perkinsstephenj)

PRINCIPAL ENGINEER, R&D, SYSTEMS, NETWORKS

I am a technology leader with a wealth of experience and broad business acumen. I have a highly diverse skill set honed by working in startups, small businesses, and enterprises. I have deep technical knowledge utilized in the R&D labs of Texas Instruments and IBM. I have envisioned and created products starting from ideation, continuing through proof of concept, and then ushered to a market product launch. I'm an entrepreneur who is technically deep and versatile across multiple verticals. I am published, patented, and networked in the industry. My research areas and interests are in:

- Communication / Writing / Presenting
- Compilers / Embedded Systems / Device Drivers / Firmware
- Deep Unix/Linux skills
- Networks, TCP/IP, eBPF
- Storage Systems / Distributed storage / CEPH
- Wireless Systems & Technology
- DEVOPS / Full Stack / C / C++ / LISP / Rust
- VMWare / Virtualization / Containers / Kubernetes
- DOCSIS / DSLAMs / IOT / Gateways, Zero Trust
- LTE / Qualcomm / MVNOs

Education

Michigan State University, East Lansing, MI

Ph.D. in Computer Science

1997

Dissertation: Noise Tolerant Compression Protocols for Wireless Environments

Chairman: Dr. Matthew Mutka

Texas A&M University, College Station, TX

M.S. in Computer Science

1991

Thesis: Graph Characteristics of Data-Flow Graphs

Chairman: Dr. Udo Pooch

Texas A&M University, College Station, TX

B.S. in Computer Science

1989

Minor: Mathematics

Professional Experience

**GIG SERVICES, INC (Parent company for: GIG WASTE MANAGEMENT, LLC,
GIG FIBER SERVICES LLC, GIG GAS SERVICES LLC) • Porter, TX • 2022 to Present**

A services company providing specialized options specific to real estate developers.

Director of Gig Services LLC

Co-founded the company in business partnership. As Director of the holding company and President of the other businesses, establish operational framework for scalability and expansion of customer base by providing neighborhood services. Implemented all aspects of startup including cash positivity.

- Developed website, service plans, support, marketing, maintenance, operations, and licensing of commercial vehicles.
- Currently in the process of standing up all three businesses before transferring management.

NETMASS INCORPORATED • Richardson, TX • 1998 to Present

A pioneer of the offsite backup and data archiving industry and possibly the first to leverage the power of the internet for dial-up based online server backup as a service in 1997. Specializing in providing internet-based safe storage and archiving technologies and services.

Principal, President, CTO

Co-founded the company in business partnership. Managed the entire reporting structure curating a culture of accountability and high performance. I currently retain ownership with no functional accountability.

- Ideated and created a business service based on online backup, then scaled, providing real value to customers.
- Developed a real solution critical to long-term success through automation and integration of processes and systems.
- Conceived and built geo-replicated datacenters for host cloud-based multi-tenant backup data utilizing colocation.
- Integrated multiple offices using IPSEC VPNs, IP Telephony, distributed file systems, CRM systems, and web and database interfaces to sales, accounting, and billing.
- Scaled HSM storage platforms at a time when disk alone was too costly for services use.
- Negotiated and closed all purchases and contracts.

CELEBRATE BAKING COMPANY, LLC • HOUSTON, TX • 2019 to Present

A 90K sq foot commercial bakery purchased in distress just before bankruptcy.

Technology and Operations / Investor

I collaborate with stakeholders and owners as an operational expert. I provide process optimization for all business functions: QA, maintenance, operations, finance, accounting & IT. I seek to continually improve operations for 11 brands of ~\$15M.

- Immediately managed operational and IT issues after the company was purchased in a state of dire distress.
- Shifted staff from a reactive/crisis mode of operation towards a proactive/productive mode of operation.
- Stabilized business operations and lowered costs by implementing repeatable processes and shared accountability.
- Stabilized the Ecommerce component, providing a significant impact to company solvency during Covid.
- Modernized with all new LAN, telephony, servers, PCs, software, and printers without assuming additional debt.

CRYSTAL SPRINGS WATER COMPANY, INC • PORTER, TX • 1999 to Present*Utility Services for Porter, Texas and the surrounding areas.***Technology and Operations Support**

I provide back-office IT and some OT technology support. In 1999, I selected their first commercial billing package and then oversaw the migration from an in-house billing system to this commercial solution. I again chose and then oversaw a billing system migration in 2021 when they outgrew the 1999 solution. I drove the research, selection, and implementation of a commercial automatic meter reading solution that improved their inground meters and the associated reading of those meters. I continue to provide technology support for this company including server virtualization, email via Microsoft 365, Cloud Services, VPN and zero-trust support, security video support, and general IT services.

MARTIN REALTY & LAND, INC • PORTER, TX • 1999 to Present*Real estate development around portions of Montgomery County, Texas.***Technology and Operations Support**

I provide back-office IT support. In 2021, I helped select a new commercial mortgage note package and then oversaw the migration from their old system to this commercial solution. I specifically wrote migration code to export their existing customer base from a no longer supported flat file database and then insert that into a Microsoft SQL Server. I continue to provide technology support for this company including server virtualization, email via Microsoft 365, Cloud Services, VPN and zero-trust support, and general IT services.

PERCEPTIVE TREKKER, LLC • Houston, TX • 2010 to Present*Consulting and Technical Services.***Principal**

Perceptive Trekker, LLC is a company that allows me to explore any business area that I desire. Through this company, I provide technical services. I also research highly available and distributed object storage solutions, high security remote access solutions, IoT development and deployment, and technical research.

SQWAQ, INC • Dallas, TX • 2018 to 2022*Full custom Bonded-LTE Hardware platform intended to support BVLOS commercial UAVs and fully autonomous platforms.***CTO / Principal / VP of Hardware and Software Engineering**

Co-founded the company in business partnership. Built and launched product and MVNO business initially targeting commercial unmanned arial vehicles. Managed a team of developers, sales associates, and founders.

- Directly involved in fund raising through angel and venture capital.
- Developed an MVNO business plan to support high margin recurring revenue.
- Engaged technology-based products to address the broad business needs, manufacturing needs, and operations of the full product life cycle. Engaged in 100% of ideation: design and board build through partnerships, security, firmware development, integration, UI, testing, manufacturing, and customer onboarding.
- Developed embedded IOT hardware & software for bonded LTE modems (Qualcomm/Sierra Wireless), with hardware supporting 6 or 12 LTE modems on a board & utilized AT and QMI interfaces. Created high performance & highly connected LTE IOT Gateway through the bonding solution allowing concurrent connections to different service providers while maintaining overlay connectivity.
- Utilized Secure Boot technologies, the Yocto project, BPF/eBPF Ansible, Redis, Git, Odoo, Linux udev, ffmpeg, lcdproc, secure over the air updates (FOTA), ZeroTier, Webmin, Prometheus, Grafana, and many Linux sub-systems.
- Created two generations of custom PCBs to house LTE modems & full custom hybrid aluminum/injection molded enclosures.
- Directly assisted with integration of the products into customer-owned platforms.
- Shaped company infrastructure to appeal to Angels as well as VCs for funding.

THE UNIVERSITY OF TEXAS DEPARTMENT OF COMPUTER SCIENCE • Dallas, TX • 2012 to 2021
A research university hosting one of the largest CS Department in the US.; initially founded in 1961 as a private research arm of TI.

Director, Executive Master in Software Engineering Program, 2017 –2021;

Full-Time Associate Professor of Instruction, 2020 – 2021;

Full-Time Assistant Professor of Instruction, 2016 –2020;

Part-Time Lecturer, 2012 – 2015

- Courses taught: CS 1335 – Computer Science I for Non-Majors, 1336 – Introduction to Programming, CS 1337 - Computer Science I, CS 3162 - Professional Responsibility in Computer Science and Software Engineering, CS3377 - C/C++ Programming in a UNIX Environment
- Recognized for teaching leadership with Presidents Teaching Award nomination
- Recognized for teaching excellence with multiple CS Teaching awards
- Selected as one of the 5 non-tenure track voting members that represent all non-tenure track faculty
- Was the Computer Science Department Amazon Web Services Liaison
- Certified AWS Instructor
- As the Director of the Executive Master program:
 - Put sustainable systems in place for reproducible processes, communication, data retention
 - restructured curriculum to meet new "in demand" courses
 - Expanded program size, even during the COVID pandemic
 - Initiated the creation of Executive Master in Computer Science (EMCS) program
- Professional Development
 - 2016 IEEE IoT World Forum, NIST Network of Things, AWS Training Academy, North Texas Smart Cities Summit, Tech Titans, 2018 DFW CIO Arena, 2018 Dallas Super Computing Show, 2019 AUVSI Exponential in Chicago, HAI Helicopter show in Atlanta, Hack UTD, and numerous campus lectures.

TEXAS INSTRUMENTS • Dallas, TX • 1984 to 1999*One of the top 10 semiconductor companies worldwide.***Member of the Technical Staff**

- Worked in the Communications Systems Engineering branch of the Digital Signal Processing Research and Development Lab. Duties included development of real-time embedded systems for communications platforms (cable modems, xDSL, and residential Ethernet). Participated in the IEEE 802.14 cable modem standards process. Participated in the Home Phone Networking Alliance (HPNA) standards process (1999).
- Designed and implemented the storage mechanism for an automatic visualization indexing system using TI's C++ object oriented database. Supervisors: Jon Courtney and Bruce Flinchbaugh (1994).
- Designed and started implementation of a real-time multiprocessor control system for an Applied Materials vapor deposition semiconductor fabrication device. This work was done as part of the Microelectronics Manufacturing Science and Technology (MMST) project. Supervisors: Richard Beaver and Dennis Draheim (1992).
- Assisted with the design of an X interface to a SUN based Computer Architecture Evaluation Toolset using C++. Supervisors: Brian Kennedy and Larry Spry (1990).
- Assisted with the design of new parallel computer architecture. Implemented some data gathering and support tools. Supervisor: Larry Spry (1988).
- Developed a graphical interface for a Common LISP environment on the TI Explorer. Supervisors: Doug Johnson and Penny Muncaster-Jewell (1987).
- Completed a Pascal to LISP translator/compiler for the specific purpose of porting TeX to the TI Explorer LISP machine. Supervisor: Penny Muncaster-Jewell (1986).
- Developed an Expert System for Rome Air Development Corporation. Demoed to Air Force members in New York. Supervisors: John Blakemore and Fried Elliot (1984-1985).

MICHIGAN STATE UNIVERSITY • East Lansing, MI • 1991-1997*Established in 1855, Michigan State University is a Land Grant, Sea Grant, and Space Grant University.***Research Assistant with the Department of Computer Science (1993-1996)**

- Consulted with TechSmith Corporation on the design and implementation of the Foray PPP Server and supporting products (1995-96).
- Implemented a worldwide low-bandwidth test bed based on a modified UNIX kernel and the Berkeley Packet Filter. Used the test bed for data collection and dissertation related analysis of low-bandwidth networks (1994-95).
- Worked on a flexible graph-object model for interoperating data and program systems (1994).
- Worked on the design and implementation of the HICLASS hierarchical classification taxonomic database system (1993).

Teaching Assistant with the Department of Computer Science (1991-1992, 1996)

- CPS-100 (Introduction to Computing)
- CPS-230 (Algorithms and Computing)
- CPS-330 (Data Structures and Programming)
- CPS-410 (Operating Systems)

TEXAS A&M UNIVERSITY • College Station, TX • 1985-1991*Established in 1871, Texas A&M University is a Land Grant, Sea Grant, and Space Grant University.***Computer Lab Operator with Department of Computer Science (1985-1986)**

- Assisted with the management of VAX Ultrix, TI Explorer, and Symbolics LISP machines.
- Provided user support for introduction computer science classes.

Computer Programmer with Department of Entomology (1986-1991)

- Managed the SUN SPARCstation network.
- Networked and managed the Symbolics LISP-machines.
- Worked in conjunction with NASA and the Texas A&M RECON group modeling closed environment life support systems for the space shuttle. This modeling was done using KEE on Symbolics LISP-machines.

Research Assistant with Academic Computing Services (1990)

- Designed and implemented a universal bitmap to TeX-PK file format conversion utility.
- Designed and implemented an Apple Macintosh to universal bitmap format conversion utility for use with the above utility.

IBM • Dallas, TX • 1989*IBM is the largest industrial research organization in the world.***Summer Intern / Computer Programmer**

- Prototyped an icon selection model for use in Office Vision.
- Developed a prototype object-oriented window platform that allows X-Windows and Presentation Manager (OS2) to be displayed with the same source code.

Publications and Papers

"Two-way broadband CATV-HFC networks: state-of-the-art and future trends", S. Perkins and A. Gatherer, Computer Networks: The International Journal of Computer and Telecommunications Networking, Elsevier Science, B.V., vol. 31, 1999, pp 313-326.

"System Software of a DSP Based Digital Subscriber Line Access Multiplexer (DSLAM)", Xiaolin Lu, Susan Yim, and Steve Perkins, Texas Instruments, Communications Systems Engineering Branch, DSP R&D, February 17, 1999

"Dependency Removal for Transport Protocol Header Compression over Noisy Channels", Stephen J. Perkins and Matt W. Mutka, IEEE International Conference on Communications, Montreal, Quebec, Canada, June 1997.

"Characteristics of Low-Bandwidth Conversations", S.J. Perkins and M.W. Mutka, Proceedings of the IEEE International Conference on Communications, vol. 3, Dallas, Texas, June, 1996, pp. 1591-1595.

"Low-Bandwidth Access: An Evaluation of Application Level Protocol Compressibility", S.J. Perkins and M.W. Mutka, Proceedings of the International Conference on Telecommunication Systems, Nashville, Tennessee, March, 1996, pp. 97-108.

"Characteristics of Low-Bandwidth Point-to-Point Conversations", S.J. Perkins and M.W. Mutka, MSU CPS technical Report, July 17, 1995.

"A New Data Model for Biological Classification", S. Jung, S. Perkins, Y. Zhong, S. Pramanik, J. Beaman, CABIOS, Vol 11, No 3, 1995, pp. 237-246.

"A Time-Step Simulation Model for a Life Support System", M.E. Makela, S.J. Perkins, H. Presig, F.E. Little, Progress Report | Regenerative Life Support Systems, NASA Space Research Center SRC-4-5873-2, March, 1988, pp. 49-72.

Patents

"Processes, articles, and packets for network path diversity in media over packet applications" (USPTO # 6,496,477)

"Integrated circuits, systems, apparatus, packets and processes utilizing path diversity for media over packet applications" (USPTO # 6,930,983)

"Sending real-time and dependent information over separate network paths" (USPTO # 7,693,062)

"Packet Circuitry Addressing Independent and Dependent Information to Different Proxies" (USPTO # 7,961,758)

"Media packet networking appliance sending diversity packets to second proxy" (USPTO # 8,396,058)

"IC generating packets containing destination, first, and second proxy addresses" (USPTO # 8,824,460)

Memberships and Interests

Network Protocols and Architectures

Highly Available and Scalable Storage

Highly Available Services

Level 4 CJIS Security Training (2021)

Mentoring of UT Dallas students

IEEE/ IEEE Computer Society Membership since 1992

Control of Automated Lighting Systems

Lighting Design (2001 to 2019)

- Jillian Edwards Concert, December 2016
- Aaron Shust Concert, December 2014
- Lauren Daigle CD Release Concert December 2014

Tri-Chair of TechTitans IoT Forum (Dec 2017 – Jan 2020)

MSU Alumni Board of Directors (Jan 2003 – Jan 2010)

Open Source Work: Next PPP Port (1992 – 1997)

American College of Surgeons - Stop the Bleed: Bleeding Control Basic (Jan 2020)

Police evidence cert

Scuba: Master Diver Training (ongoing)

Private Pilot - Cessna Training Solo Flights (2003)

Skydiving

Avid Motorcycle Rider