

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, LLC,

Petitioner,

v.

DYNAPASS IP HOLDINGS LLC,

Patent Owner

IPR2023-00425

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

**DECLARATION OF RAJEEV SURATI, IN SUPPORT OF
DYNAPASS IP HOLDINGS LLC'S PATENT OWNER RESPONSE**

I, Rajeev Surati, declare as follows:

1. I make this declaration based upon my own personal knowledge and, if called upon to testify, would testify competently to the matters contained herein.

2. I have been asked to render opinions in *inter partes* review proceeding IPR2023-00425, regarding claims 1 and 3-6 (the “Challenged Claims”) of U.S. Patent No. 6,993,658 (Ex. 1001, the “’658 Patent”).

3. This declaration is a statement of my opinions on issues related to the patentability of the Challenged Claims.

4. I am being compensated at my usual rate. My compensation is in no way related to the outcome of this case.

I. BACKGROUND AND QUALIFICATIONS

5. I, Rajeev Surati, have been retained by counsel for Dynapass IP Holdings LLC (“Patent Owner”) as an expert in *Unified Patents, LLC v. Dynapass IP Holdings LLC*, IPR2023-00425.

6. In formulating my opinions, I have relied on my knowledge, training, and experience in the relevant field, which I will summarize briefly here. In addition, my *curriculum vitae* (CV) is attached to this declaration (Ex. 2004).

7. I hold a Doctor of Philosophy in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology (awarded in 1999) with a Grade Point Average of 5.0/5.0. I obtained a Master of Science in Electrical

Engineering and Computer Science from the Massachusetts Institute of Technology (awarded in 1995) with a Grade Point Average of 5.0/5.0. I have a Bachelor of Science in Electrical Engineering from the Massachusetts Institute of Technology (awarded 1992) and graduated with a Grade Point Average of 4.9/5.0.

8. My Ph.D. thesis was entitled “Scalable Self-Calibrating Technology for Large Scale Displays.” My master’s thesis was entitled “Practical Partial Evaluation.” My undergraduate thesis, which I received the MIT EECS’s William A. Martin thesis prize for best undergraduate thesis, was entitled “A Parallelizing Compiler based on Partial Evaluation.” Lastly, I was awarded the highly selective Department of Energy’s Computational Science Fellowship in 1995, which funded my Ph.D. studies.

9. Between 1989 and 1999 I was employed as a researcher/programmer at the MIT Artificial Intelligence Lab. At the lab, I worked for Thomas F. Knight Jr., Ph.D. He is one of the noted inventors of the first bit-mapped displays for computers, a core programmer on the ITS (intelligent time-sharing operating system), creator of several innovations in VLSI, and most recently noted as being one of the grandfathers of synthetic biology. I also worked for Professor Anant Agarwal on parallel computing and Professors Hal Abelson and Gerald J. Sussman on parallel and scientific computing.

10. In 1990 I learned and used EPROM's for the first time in a Computer Architecture course and learned the labor-intensive process used to erase and reprogram them using UV and EPROM programmers.

11. In 1996, I began working on a Ph.D. thesis related to the display of multimedia across large displays. My Ph.D. thesis system was a special kind of display allowing one to create ultra-high-resolution displays composed of multiple projectors tiled with a slight overlap. A camera-based feedback system is used to create an inverse map to drive the system such that a person would only see a continuous, seamless display with no bezel or overlap. What content and how to drive it onto the display was a topic I became familiar with. Also, at this time, several interactive TV projects were going on at MIT, which I had exposure to from this vantage, especially concerning the idea that these large displays would be in the living rooms of the future. Thus, I became familiar with content encoding/decoding, user interfaces for driving large displays, multimedia content storage, high-resolution imagery, networks, recording, GPUs, storage of content, etc.

12. In 2002, MIT was awarded U.S. Patent 6,456,339, entitled "Super-resolution Display," for my Ph.D. work. Today this technology is better known as automatic calibration for projection mapping. My experience, along with a patent I developed and licensed based on my Ph.D. thesis, were used to create a new startup

company called Scalable Display Technologies that works with a variety of Pro AV display companies' products.

13. While at MIT pursuing my doctorate, I started a company called Flash Communications in 1997, which invented an instant messaging platform focused on enterprise needs. It had its basis from my having observed the popularity at MIT of the Zephyr Instant Messaging Service from 1988 onwards. Given this enterprise focus, Microsoft soon acquired the company in 1998. We built both a client and server product, and the basic protocol we invented became the basis of the well-known XMPP protocol that was widely used in the mid-2000s among instant messaging providers. I worked on developing both the client and server products and particularly dealt with many, if not all, of the issues one might have to face when implementing contact lists. Notably I implemented the login authorization system for this system.

14. Upon graduation, I joined Microsoft (as was required by Microsoft in the acquisition of Flash Communications) and worked on both client and server technologies related to instant messaging, covering both the Microsoft Exchange Instant Messaging product that was released in 2000 and MSN Messenger. At Microsoft, I also worked on the client and server side of the products.

15. At Microsoft, I participated in development of the Instant Messaging and Presence Protocol (IMPP), which was at least partially derived from a similar

protocol that I worked on at Flash. The IMPP protocol was later incorporated into the Extensible Messaging and Presence Protocol (XMPP) protocol that was used widely for instant messaging by Microsoft, Google, Cisco, Jabber, and several others.

16. As this XMPP adoption was going on, there was further internal discussion regarding the Session Initiation Protocol (SIP) protocol, which was eventually adopted more broadly by Microsoft for Instant Messaging. The SIP protocol is used for signaling and controlling multimedia communication sessions in applications of Internet telephony for voice and video calls, instant messaging over Internet Protocol (IP) networks, as well as mobile phone calling over LTE (VoLTE). While working at Flash and Microsoft, I was personally responsible for developing source code for parsing and processing input messages and generating output messages in accordance with the above-described protocols, and thus I have an extensive working knowledge of many different protocols used in multimedia communications systems. Furthermore, I worked on an SDK integrating the Exchange Servers with the MSN Servers.

17. In 2002, I served as a technical consultant for Cordant Communication, which was founded for the purpose of archiving instant messages. During this time, I also served as an informal adviser to IMLogic, which also worked on message archiving. Later in 2007, I served as a technical adviser to Unify Square, which built

software to manage Microsoft telephony and messaging solutions deployed in Fortune 500 companies. Unify Square was recently sold to Unisys.

18. From 2000 to 2007, I cofounded, led, and sold a business called photo.net to Namemedia, which is now part of GoDaddy.com. In 2000, while running the site, I worked on many features including a chat feature, a WAP interface to photo.net, and a rich user interface based on JavaScript. Photo.net for a time in early 2000 was considered a top 1,000 website so it received large amounts of traffic. Having built the site from running on a single computer that I installed in a datacenter to a full rack of computers in that data center, I became very familiar with the careful design and programming one needs to employ in building and maintaining such systems. I became intimately familiar with implementing file systems for use with multimedia and super high performance image encoding/decoding systems as well as real time delivery of high bandwidth content.

19. At photo.net, we prototyped many fundamental Internet community features such as photo sharing, social networking, and memberships in the late 1990s and early 2000s. This system was written on top of Oracle SQL Database and had to serve up many millions of web pages a day (corresponding to millions of records), with high volume inserts and also incorporated an ecommerce system used for billing of subscriptions, tracking users etc. I spent seven years running the site both writing new features driven by the Oracle SQL database and maintaining tables with

many millions of records being generated. I also served as the database administrator for seven years, which provided me with personal and extensive operational experience running such a system, dealing with database query speed-up and more mundane day-to-day issues regarding maintaining relational databases such as backups, etc.

20. Again at photo.net I maintained and implemented the login system.

21. I also worked with the team at ArsDigita including Dr. Philip Greenspun, who created the photo.net site as a hobby in 1993 while we were at MIT, and who asked me to cofound the business with him in 1999 when I came back from Microsoft. ArsDigita built public open source community web site creation tools similar to what people today call Drupal on which many thousands of websites were built, including both enterprise and consumer web sites. ArsDigita's product came out of the work to develop photo.net, and photo.net served as a prime example site of one using the ArsDigita System as its underlying content management system.

22. The photo sharing system on photo.net was built on top of a photo database engine called PhotoDB including features like key word tagging, folder, and even making custom fields that users could customize for making their own personal tables. I rebuilt and maintained much of the user interface for this in 2001 until the site was sold.

23. Because photo.net was focused on high-end amateur photographers, I worked with many consumer electronics manufacturers in the digital camera business. There, I implemented a photo sharing system involving the delivery of multimedia content. Additionally, I worked on e-commerce capabilities that involved some product configuration options. In running photo.net, I became intimately familiar with implementing file systems for use with multimedia and super high performance image encoding/decoding systems as well as real time delivery of high bandwidth content.

24. Messaging and broadcasting content were a core part of the offering of the site, and I managed the implementation and hosting aspect of setting up and running various SMTP, MTA, WAP, and SMS servers to enable communication with our user base. In that regard, WAP PUSH, which is a relevant protocol to messaging, was something I worked on as well at the time.

25. In 2001, I became involved with helping a rich user interface (UI) web company, Nexaweb, as both an investor and advisor. In that role, I worked on the underlying infrastructure for a device independent (mobile device, PC, etc.) way to write UIs for web application utilizing Java as a rendering engine backed by web server backend. Underlying that technology required providing server pushes over HTTP. At that time JavaScript could provide a UI but it was not standardized across

browsers, which made it hard to implement reliable systems that worked across browsers—especially ones that required server push underneath it.

26. In 2004, I founded Scalable Display Technologies (SDT) and I have been the President and Chairman of the company since the founding. Among its operations, SDT operates in the Audio Video domain and has licensed software and firmware to various companies including Hitachi and NEC. I also wrote a network synchronized media playback system involving encoding and decoding of video and audio content as well as real time recording and video capture, a product known as “ScalablePlayer.” I was also involved in building a network architecture using both broadcast and point-to-point communication mechanisms.

27. Also, as detailed in my attached CV, I am an inventor of subject matter in approximately 10 U.S. Patents. I have also received additional patents, including: U.S. Patent No. 8,817,111, entitled “System and method of calibrating a display system free of variation in system input resolution”; U.S. Patent No. 8,994,757, “System and method for providing improved display quality by display adjustment and image processing using optical feedback”; U.S. Patent No. 9,215,455, “System and method of calibrating a display system free of variation in system input resolution”; U.S. Patent No. 9,369,683, “System and method for calibrating a display system using manual and semi-manual techniques”; and U.S. Patent No. 9,497,447,

“System and method for color and intensity calibrating of a display system for practical usage.”

28. I am co-inventor of patented technology related to instant messaging upon I which focused on technology related to U.S. Patent No. 5,943,478 and associated technology that I had developed related to pop-up, two-way messaging over the Internet. While at Microsoft, I was an inventor on several patents including: U.S. Patent No. 6,260,148 relating to methods and systems for message forwarding and property notifications using electronic subscriptions; and U.S. Patent Nos. 6,415,318 and 6,604,133 relating to inter-enterprise messaging systems using bridgehead servers. Aspects of these patents relate specifically to messaging and notification technology in telecommunications systems.

29. I am on the advisory boards of several technology companies, including: Paneve, which develops general purpose ASICs coupled with compiler technology; Nexaweb, which develops real-time web application frameworks using HTTPS; Antix Labs, which develops compiler technology for a universal gaming platform; and Permabit, which develops content addressable storage.

30. I have received several awards for my contributions as an inventor and entrepreneur, including the Global Indus. Technovator Award 2009 and Laureate of 2009 Computer World Honors Program.

31. In parallel with my work at SDT, I lectured at MIT on many subjects including the Android operating system, and I worked with a group of students on developing mobile applications for Android in 2008 with Rich Miner, who is a co-founder of Android. Many students created applications involving Google Maps and localization, so I was familiar with these. I also served as a lecturer and mentor at MIT Play Labs, which was an incubator for augmented reality (AR) and virtual reality (VR) software for mobile handsets and headset applications. Notably in addition to mobile handsets, Android runs on the Oculus headset. As part of that program, I worked with several startup companies on mobile applications including one that developed applications for Telegram, which is a cross-platform, cloud-based instant messaging system.

32. Since 2014, I have been working as an independent consultant for several companies including NEC, Hitachi, Hi Marley, and Estee Lauder.

33. In 2018, I became a senior partner at nCent Labs. In this role, I consulted on the development of an incentive market-based platform for block chains and cryptocurrency. Part of my work at nCent Labs focused on the development of SMS messaging applications for the nCent platform. In my role there I also implemented an OTP based user authorization system.

34. Between 2019 and 2020, I served as a Technical Lead of the Skunkworks at Hydrow, which is a startup company that develops indoor rowing

machines. In this role, I worked on special projects including development of a virtual reality experience using Magic Leap and Oculus to immerse users in a world of team-based rowing crew on a scull based on virtual reality (VR) cinematography.

35. I have published numerous papers on subjects relating to computing systems, computer network communications, databases, and other subjects within the realm of electrical and computer engineering.

36. In 2020, I started a company called Skyline Nav AI Inc. that develops technology using visual location (using skyline) to geo-locate the place a picture was taken as an alternative to GPS. There I have built and maintained a login authentication system for our app skyline nav for Android Tactical Assault Kit (ATAK) a US Military program for GIS based collaboration in the field. I implemented an OTP based authentication system.

37. Over the past decade, I have served as a technical consultant and expert witness on matters relating to numerous patent infringement cases. In the course of this work, I have provided consulting services to a wide variety of technology companies including BritishTelecom, Apple, IBM, Philips, Shopify, Zillow, Polaris Powered Technologies, Amazon, Salesforce, Hitachi, Slack, Harris Teeter, and others.

38. I have been teaching a Big Data class at Harvard Medical School one month of every year since 2018. The name of the class is “Computationally Enabled Medicine.”

39. Finally, for the last 10 years I have served as an angel investor and also as a mentor for startup companies as part of different programs at MIT.

40. Lastly over the last 35 years as a practicing computer scientist and engineer I have regularly interacted with login authentication systems including OTP based ones. RSA authentication based ones as well as other public and private key based ones.

41. As such, I am qualified to provide opinions regarding the state of the art at the effective filing date of the '658 Patent (which I understand to be March 6, 2000) and how a person of ordinary skill in the art (“POSITA”) at that time would have interpreted and understood the '658 Patent.

42. I am being compensated for my work and any travel expenses in connection with this proceeding at my standard consulting rates. My compensation is in no way dependent on or contingent on the outcome of my analysis or opinions rendered in this proceeding and is in no way dependent on or contingent on the results of these or any other proceedings relating to the above-captioned patent.

43. Although I am not rendering an opinion about the level of skill of a POSITA proffered by Petitioner, based on my professional experience, I have an

understanding of the capabilities of a POSITA (as such a POSITA is defined by Petitioner). Over the course of my career, I have supervised and directed many such persons. Additionally, I myself, at the time the '658 Patent was filed and at its priority date, qualified as at least a POSITA.

II. MATERIALS CONSIDERED

44. In preparing this declaration, I reviewed the '658 Patent, including its claims in view of its specification, the prosecution history of the '658 Patent, and various prior art and technical references from the time of the invention.

45. In addition, in preparing this declaration, I have reviewed all of the papers and exhibits in the record for *inter partes* review proceeding IPR2023-00425.

III. LEGAL UNDERSTANDING

46. I have worked with counsel for Patent Owner in the preparation of this Declaration. Nevertheless, the opinions, statements, and conclusions offered in this Declaration are purely my own and were neither suggested nor indicated in any way by counsel or anyone other than myself. I confirmed with counsel my understanding that the term "obvious," as used in the Petitions addressed herein and as a general matter under United States law, refers to subject matter that would have occurred to a POSITA to which the '658 Patent is directed without inventive or creative thought. That which is obvious, it is my understanding, flows naturally from the art and the

education one of skill practicing in that art would have had in the relevant time frame, which for the '658 Patent is 2000.

A. Obviousness

47. I understand that a patent claim can be invalid under 35 U.S.C. § 103 if the claimed subject matter would have been “obvious” to a person of ordinary skill in the art as of the priority date of the patent based upon one or more prior art references. I understand that an obviousness analysis should consider each of the following so-called “Graham factors”: (1) the scope and content of the prior art; (2) the differences between the claims and the prior art; (3) the level of ordinary skill in the pertinent art; and (4) secondary considerations, if any (such as unexpected results, commercial success, long-felt but unsolved needs, failure of others, copying by others, licensing, and skepticism of experts).

48. I understand that a conclusion of obviousness may be based upon either a single prior art reference or a combination of prior art references. However, I understand that merely demonstrating that each of the claim elements was, independently, known in the prior art does not prove that a claim composed of several known elements is obvious. In other words, I have been informed that obviousness requires more than a mere showing that the prior art includes separate references covering each limitation in a claim. Rather, obviousness requires the additional showing that a person of ordinary skill at the time of the invention would

have selected and combined those elements in the normal course of research and development to yield the claimed invention.

49. Moreover, I understand that it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in a way the claimed new invention does.

50. I further understand that, to determine obviousness, courts look to the interrelated teachings of multiple patents or other prior art references, the effects of demands known to the design community or present in the marketplace, and the background knowledge possessed by a person having ordinary skill in the art.

51. I also understand that, in determining whether a combination of prior art references renders a claim obvious, it may be helpful to consider whether there is some teaching, suggestion, or motivation to combine the references and a reasonable expectation of success in doing so. I understand, however, that the teaching, suggestion, or motivation to combine inquiry is not required and may not be relied upon in lieu of the obviousness analysis outlined above.

52. I understand that the following exemplary rationales may lead to a conclusion of obviousness: the combination of prior art elements according to known methods to yield predictable results; the substitution of one known element for another to obtain predictable results; and the use of known techniques to improve similar devices in the same way.

53. However, a claim is not obvious if the improvement is more than the predictable use of prior art elements according to their established functions. Similarly, a claim is not obvious if the application of a known technique is beyond the level of ordinary skill in the art.

54. Further, when the prior art teaches away from combining certain known elements, discovery of successful means of combining them is not obvious. I understand that similar subject matter may not be sufficient motivation for a person of skill in the art to combine references if the references have conflicting elements.

55. I understand that, in order to be used in an obviousness combination, a prior art reference must be “analogous.” I understand that two separate tests define the scope of analogous prior art: (1) whether the art is from the same field of endeavor, regardless of the problem addressed; and (2) if the reference is not within the field of the inventor’s endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved. In regard to test (2), the problems to which both the reference and the claimed invention relate must be identified and compared. I also understand that Petitioner has the burden of showing a cited reference is analogous art.

56. I understand that obviousness of a patent claim cannot properly be established through hindsight, and that elements from different prior art references, or different embodiments of a single prior art reference, cannot be selected to create

the claimed invention using the invention itself as a roadmap. I understand that the claimed invention as a whole must be compared to the prior art as a whole, and courts must avoid aggregating pieces of prior art through hindsight that would not have been combined absent the inventors' insight.

57. I understand that obviousness is not established by simply combining previously known elements from the prior art. A patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. An invention is unpatentable as obvious if the differences between the patented subject matter and the prior art would have been obvious at the time of invention to a person of ordinary skill in the art.

58. I understand that obviousness of a patent cannot properly be established by mere conclusory statements. Instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. When an expert opines that all the elements of a claim disparately exist in the prior art, the expert should provide the rationale to combine the disparate references. A reason for combining disparate prior art references is a critical component of an obviousness analysis. The obviousness analysis should be made explicit and needs to provide an articulated reasoning with some rational underpinning to identify the reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed invention does.

59. I also understand that inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known. This is another reason why merely pointing to the elements being known in the art in separate locations is not the end of the obviousness inquiry.

60. I understand that technical experts may testify to matters like the level of skill in the art at the time of the invention and what a POSITA might find obvious in light of the prior art without addressing objective indicia of non-obviousness. However, where an expert purports to testify not just to certain factual components underlying the obviousness inquiry, but to the ultimate question of obviousness, the expert must consider all factors relevant to that ultimate question, including all objective evidence of non-obviousness. Accordingly, I have undertaken such considerations here.

61. I understand that, to render obvious a patent claim the prior art references must be enabling. That is, the references must provide sufficient information to allow one skilled in the art to practice what is disclosed without undue experimentation. I understand that, while a prior art reference may support any finding apparent to a person of ordinary skill in the art, prior art references that address different problems may not, depending on the art and circumstances, support an inference that the POSITA would consult both of them simultaneously.

B. Secondary Considerations

62. I understand that one of the so-called *Graham* factors that must be considered in determining obviousness is the existence of any secondary considerations, which tend to show that a patent claim is not obvious. Such secondary considerations of non-obviousness of a patent include (1) long-felt and unmet need in the art that was satisfied by the claimed invention of the patent; (2) failure of others to achieve the results of the claimed invention; (3) commercial success or lack thereof of the products and processes covered by the claimed invention; (4) deliberate copying of the claimed invention by others in the field; (5) taking of licenses under the patent by others; (6) whether the claimed invention was contrary to the accepted wisdom of the prior art; (7) expression of disbelief or skepticism by those skilled in the art upon learning of the claimed invention; (8) unexpected results achieved by the claimed invention; (9) praise of the claimed invention by others skilled in the art; and (10) lack of contemporaneous and independent invention by others.

63. I understand that each of these considerations may form an independent basis for non-obviousness of a patent. I also understand that the fact that another person simultaneously and independently created the same invention claimed in an asserted patent can serve as an indication that the invention was obvious.

64. I also have been informed by counsel that there must be a nexus between any such secondary considerations and the claimed invention.

IV. CLAIM CONSTRUCTION

65. I reviewed the comments in the Petition and Mr. McNair's Expert Declaration (Ex. 1003) pertaining to "construction of the claims" of the '658 Patent. My understanding is simply that, in the absence of a specific controversy, one arrives at the appropriate "construction" or definition of what is embraced by the claims of the '658 Patent and what is excluded by those claims by a reading of the '658 Patent and arriving at what, based on that reading, the inventor of the claimed subject matter intended to protect as her or his invention.

66. In my opinion, the plain language of claim 5 requires activation of account access in response to generation of the claimed "new password." The relevant portions of claim 5 are reproduced below:

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;

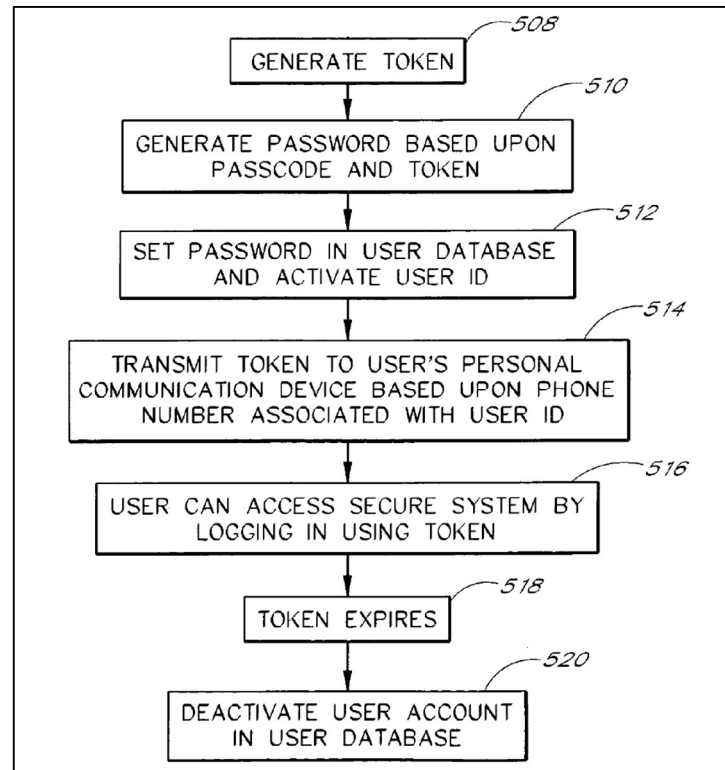
* * * * *

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.

Ex. 1001 at 12:27-47 (emphasis added). A POSITA would interpret this to mean the “control module” creates a “new password.” Then it sets a “password” to be the “new password” that was created by the “control module.” *Id.* at 12:27-33. The “authentication module” claim element recites “the password” several times. *See id.* at 12:37-47. The “a password” term recited in the “control module” claim element provides the antecedent basis for “the password” term in the “authentication module” claim element. *See id.* at 12:27-47. Thus, when the claim recites “wherein the authentication module activates access to the account in response to the password,” it is referring to the “a password” that is introduced in the “control module” claim element. *See id.* In my opinion, it follows from the plain language of the claim, that creation of that password is a prerequisite to the “authentication module activat[ing] access to the account in response to the password.” *See id.*

67. That same process is depicted, for example, in Figure 5 of the ’658 Patent, which is reproduced in pertinent part below:



Ex. 1001, Fig. 5. The password is generated in step 512, which causes activation of access to the user's account in step 512. *See id.* Accordingly, in my opinion, the plain language of claim 5 requires activation of account access in response to generation of the claimed "new password."

V. OPINIONS REGARDING OBVIOUSNESS

68. Petitioner challenges independent claims 1 and 3-6 of the '658 Patent (the "Challenged Claims").

69. In my opinion, as described below, Petitioner has not established by a preponderance of the evidence that the challenged claims are unpatentable.

A. Ground 1 – *Veneklase* and *Jonsson* Do Not Render Claim 5 Obvious

70. In my opinion, *Veneklase* and *Jonsson* (the “Ground 1 References”) do not render obvious independent claim 5.

1. Independent Claim 5

71. In my opinion, the combination of *Veneklase* and *Jonsson* does not render obvious independent claim 5 because the combination does not teach or suggest the following elements of the claim.

a. Claim element [5.3]

72. Claim element [5.3] 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.” Petitioner mapped *Veneklase*’s “user/password check” module to the claimed “control module” (see Pet., pp. 26-27), but concedes that *Veneklase* does not disclose this claim element. See Pet., p. 28 (*Veneklase* “does not disclose creating a new password based on those two items.”). Petitioner argues that the combined teachings of *Veneklase* and *Jonsson* meet the requirements of claim element [5.3]. See Pet., pp. 28-34. But in my opinion, Petitioner’s proposed combination fails to support a conclusion of obviousness for multiple reasons.

73. Petitioner argues that “*Veneklase* teaches a system which a user inputs a password known beforehand, receives a randomly generated previously-unknown code, and then inputs that [randomly generated code] for authentication purposes.” Pet. at 31 (citing Ex. 1005, 7:52-8:27). In other words, “*Veneklase*’s system allows for authentication through user input of a known and unknown code at separate times in a two-step process.” *Id.* (emphasis added).

74. *Jonsson* discloses an authentication process in which a “personal unit 20 receives an authentication challenge code, it prompts the user to input a PIN or other identifying information, and generates a response code by an algorithm having the challenge code . . . and the PIN.” See Ex. 1006, 9:1-13. This response code is then “displayed on a display unit [of personal unit 20] for manual input to [user’s] terminal,” and then transmitted from the user’s terminal to the system for comparison with an expected response code. *Id.*, 9:26-35.

75. Petitioner’s proposed combination includes replacing *Veneklase*’s two-step authentication process (i.e., user transmission of *Veneklase*’s password, and subsequent user transmission of *Veneklase*’s random code) with the single step in *Jonsson* (i.e., user transmission of *Jonsson*’s response code). See Pet. at 28 (“*Veneklase* teaches an authentication system in which the user inputs both a token . . . and a passcode . . . it would have been obvious to combine those two steps and instead create a new password based on both of them”) (emphasis added), 31 (“A

POSITA would have been motivated to make such a combination because having only the one password transmitted via the computer system is more efficient and secure . . . *Veneklase's* system allows for authentication through user input of a known and unknown code at separate times in a two-step process, while a POSITA would look to *Jonsson* because it would provide the added benefit of reducing the steps to a single step") (emphasis added), 34 ("A POSITA would have had a reasonable expectation of success in modifying *Veneklase's* authentication system, which requires the use of both a known password and a previously-unknown randomly generated code, to create a new password based on those two values . . . because doing so would have merely made two steps into one without requiring any additional hardware.") (emphasis added).

76. But in my opinion, modifying *Veneklase's* system by eliminating the two-step authentication process would violate *Veneklase's* principle of operation. *Veneklase's* two-step authentication process "ensure[s] that an authorized user of a computer system is notified that someone or something is seeking access to the computer system with his or her password . . . [and] allows for multiple levels of security before access to the computer system is achieved and provides enhanced security over the prior art." Ex. 1005, 7:16-28. Accordingly, in my opinion, this two-step authentication process is a core/fundamental feature of *Veneklase's* principle of operation, and a POSITA would not seek to remove these steps as

Petitioner proposes. *See id.* In my opinion, the proposed modification of *Veneklase* is far too drastic to be considered obvious, and thus the combination of *Veneklase* and *Jonsson* fails to render claim 5 obvious.

77. Petitioner also argues that “a POSITA would have been motivated to make such a combination because implementing *Veneklase*’s authentication system with the algorithm of *Jonsson*’s system provides an additional layer of security . . . a POSITA would have been motivated to use an algorithm for creating a new password based on the known password and the previously-unknown randomly generated code, such as described in *Jonsson*, to provide additional security.” Pet., pp. 31-32 (emphasis added). But Petitioner argued that a POSITA would have been motivated to reduce the number of steps in *Veneklase*. *See* Pet. at 31 (“a POSITA would look to *Jonsson* because it would provide the added benefit of reducing the steps to a single step.”) (emphasis added). Moreover, in my opinion, *Veneklase*’s two-step authentication process already “allows for multiple levels of security before access to the computer system is achieved.” Ex. 1005, 7:26-27. For example, *Veneklase*’s system does not transmit the randomly generated code to the user until *Veneklase*’s password is received from the user (i.e., the first step in the two-step authentication process) and “cross reference[d] . . . against a pager phone number list resident within the user table 414.” Ex. 1005, 8:2-5. Petitioner concedes as much. *See* Pet., p. 42 (“*Veneklase* discloses that this system is implemented only when the

password is found within the master password list.”) (emphasis added). *Veneklase* identifies the two-step process as providing a security benefit: should a hacker or other unauthorized user gain access to the user’s password, this first step in *Veneklase*’s system also has the added bonus of notifying the user “that someone or something is seeking access to the computer system with his or her password.” See Ex. 1005, 7:16-21.

78. Petitioner’s proposed combination dismantles *Veneklase*’s existing multi-level security by discarding user transmission of the password and thus discarding the cross-referencing security feature and notification feature. In my opinion, Petitioner provides zero evidence that the security of its proposed combination is superior to the existing multi-layer/level security in *Veneklase*. Accordingly, there is no motivation to combine *Veneklase* and *Jonsson*.

79. Petitioner also argues that combining the algorithm of *Jonsson* with *Veneklase* would thwart “SIM swapping” attacks. Pet., p.32. The Petition contends that “SIM swapping is a well-known trick of hackers in which they contact your service provider and activate a new SIM card on a different device in order to receive the user’s authentication token.” *Id.* at 32. It further contends that SIM swapping “would not work in the combined system, because [hackers] would need access to the device containing the correct algorithm.” *Id.* But as I discuss below regarding claim element [5.4], the combined system would be more prone to DOS attacks by

hackers, which in my opinion, would lead a POSITA away from the proposed combination. Further, in my opinion, SIM swapping would also not work in *Veneklase's* existing system because the hackers would still need *Veneklase's* password. For these reasons, in my opinion, the combined system is not superior to *Veneklase* in terms of security. Accordingly, in my opinion, a POSITA would not be motivated to combine *Veneklase* and *Jonsson*.

80. Petitioner also argues that “*Veneklase* explicitly provides a teaching, suggestion, and motivation for combining it with an authentication system that uses an algorithm, such as taught in *Jonsson*, because it explicitly discloses embodiments in which datastreams are encoded and decoded using algorithms for additional security.” Pet., p. 32 (citing Ex. 1005, 9:26-10:11). The Petition fails to describe that “algorithm” in any detail, which is not surprising, because the section of *Veneklase* cited by Petitioner does not pertain to an algorithm.

81. The portion of *Veneklase* cited by Petitioner discloses “a commercially available one input and two channel output time division or statistical multiplexor which samples the bits of [] data and places, in a certain predetermined manner (e.g. alternately) some of the [] data bits onto the first communications channel 76 [for transmission to a receiver] and some of the [] data bits onto the second communications channel 78 [for transmission to the receiver].” Ex. 1005, 8:35-41. The receiver “contains [a] ‘mirror image’ of the algorithm used to divide the data

stream . . . In this manner, the data from each of the channels 76,78 is reconstituted [at the receiver] onto single channel 89.” Ex. 1005, 8:53-57. In other words, the “algorithm” disclosed in *Veneklase* does nothing more than split (i.e., multiplex) data streams across multiple channels, without any description of generating or modifying the content of the data. *See id.* By contrast, the “algorithm” disclosed in *Jonsson* “generates a response code by an algorithm having the challenge code, an internal security code and the PIN as variable [*sic*].” Ex. 1006, 9:9-13. Thus, the “algorithm” disclosed by *Veneklase* is not related to the authentication algorithm disclosed by *Jonsson*. Accordingly, in my opinion, this algorithm disclosed by *Veneklase* is not “explicit[] . . . teaching, suggestion, and motivation for combining” *Veneklase* with *Jonsson*’s algorithm, as Petitioner argues. Pet., p. 32.

82. In view of the above, in my opinion, the combination of *Veneklase* and *Jonsson* fails to teach or suggest claim element [5.3], and thus fails to render claim 5 obvious.

b. Claim element [5.4]

83. Claim element [5.4] recites “a communication module configured to transmit the token to the personal communication device through the cell phone network.” Petitioner argues that this limitation is met by the “automatic phone/pager dialer 418” in *Veneklase*. Pet., p. 35.

84. Petitioner argued that “*Veneklase* teaches a system which a user inputs a password known beforehand, receives a randomly generated previously-unknown code, and then inputs that [randomly generated code] for authentication purposes.” Pet. at 31 (citing Ex. 1005, 7:52-8:27). In other words, “*Veneklase*’s system allows for authentication through user input of a known and unknown code at separate times in a two-step process.” *Id.* (emphasis added). *Veneklase*’s system uses the received password (i.e., the first step in the two-step process) to lookup the user’s phone number and transmit the randomly generated code to the user. *See* Ex. 1005, 8:2-15 (*Veneklase*’s system “cross references the received password [] against a pager phone number list . . . [the randomly generated] code along with the authorized user’s pager number [is passed] to the commercially available and conventional automatic dialer . . . [which] transmits the code to the user’s pager.”). *See also* Ex. 1005, 6:10-37 (“analyzing means 12 then checks and/or compares this first received password with a master password list . . . each authorized password 202, contained in this master password list 200, has a unique first entry 204 associated with it and which identifies the name of the authorized user who has been assigned that corresponding password and at least one telephone number 206 . . . associated with the identified user. If the received password matches an entry of the master password list,” a randomly generated code is transmitted “to the individual 85 associated with the received password 202 in the master password list.”) (emphasis added); Pet. at 35.

85. Accordingly, *Veneklase's* system (1) receives the password from the user (first step in two-step authentication process), (2) uses the received password to lookup the phone number associated with the user, (3) generates a random code, (4) transmits the random code to the user's pager using the phone number identified from the received password, and then (5) receives the random code from the user (second step in two-step authentication process). *See* Ex. 1005, 6:10-37, 8:1-26. For the user to be authenticated, the received random code from the user must match the generated random code. *Id.*

86. As discussed above in reference to claim element [5.3], Petitioner's proposed combination includes replacing *Veneklase's* two-step authentication process (i.e., user transmission of *Veneklase's* password, and subsequent user transmission of *Veneklase's* random code) with the single step in *Jonsson* (i.e., user transmission of *Jonsson's* response code). Accordingly, following Petitioner's proposed modification to *Veneklase*, the user in *Veneklase* no longer transmits the password to the system (i.e., the first step in *Veneklase's* two-step authentication process is abolished in the proposed modification). But as discussed above, *Veneklase* needs the received password to lookup the phone number of the user in a password list and transmit the randomly generated code to the user's pager, as conceded by Petitioner. *See* Pet., p. 42 ("*Veneklase* discloses that this system is implemented only when the password is found within the master password list.")

(emphasis added). The Petition is silent on how, following the proposed modification to *Veneklase* which abolishes user transmission of *Veneklase*'s password, the user's phone number will be identified, and thus how the randomly generated code will be transmitted to the user's pager (steps (2) and (4), discussed above). In my opinion, with *Veneklase*'s modified system being unable to search the password list for a phone number, and thus unable to transmit the randomly generated code to the user's pager, *Veneklase*'s modified system is inoperative. Thus, in my opinion, there is no motivation for the proposed modification.

87. It is my understanding that the Board rejected this argument in the Institution Decision. It is also my understanding that the Board believes the user's device in the proposed combination is being identified according to the teachings of *Jonsson* and that the combination does not require looking up the user's phone number

88. In my opinion, *Jonsson*'s teachings still require looking up the user's phone number. That is because *Jonsson*'s "personal unit 20 can be essentially a conventional pager which is modified" (Ex. 1006, 6:31-32) and connected to an "authentication challenge network 28 . . . such as a public or private telephone network." Ex. 1006, 6:3-6. In my opinion, a POSITA would understand this to mean *Jonsson*'s "personal unit 20" has a phone number and the phone number must be used to transmit to the "personal unit 20."

89. Further, as discussed above regarding claim element [5.3], Petitioner’s motivation for combining *Veneklase* and *Jonsson* includes “reducing the steps to a single step and thus reducing the amount of time required for the authentication process.” Pet., p. 31. But in my opinion, if the proposed combination still relies on *Jonsson*’s teachings to identify the user’s device, then the overall authentication process in the proposed combination still has two steps: (1) the user transmits *Jonsson*’s “authentication request” to the system (to trigger generation of the “challenge code”) (Ex. 1006, 9:1-4, 10:18-20, Fig. 3), and then (2) the user transmits the “response code” (Ex. 1006, 9:26-30, 11:4-13, Fig. 3) to the system. Thus, in my opinion, Petitioner’s rationale for combining *Veneklase* and *Jonsson* is not actually realized, and a POSITA would not be motivated to execute the proposed combination.

90. According to Petitioner, a “POSITA would have been motivated to make such a combination [of *Veneklase* and *Jonsson*] because having only one password transmitted via the computer system is more efficient and secure.” Pet., p. 31 (emphasis added). But in my opinion, if the proposed combination still relies on *Jonsson*’s teachings to identify the user’s device, then Petitioner is assuming that *Jonsson*’s “authentication request” is not a password (i.e., not a secret). In my opinion, if *Jonsson*’s “authentication request” is not a password, then the proposed combination is open to denial of service attacks (DoS). This is a flaw in *Jonsson*’s

architecture and a flaw in the proposed combination. In contrast, *Veneklase*'s system with its two passwords does not suffer from this flaw or at least is less susceptible to a DoS attack. Accordingly, in my opinion, there is no motivation to combine *Veneklase* and *Jonsson* as proposed by Petitioner.

91. In view of the above, in my opinion, Petitioner fails to show that the combination of *Veneklase* and *Jonsson* teaches or suggests claim element [5.4], and thus fails to show that the combination of *Veneklase* and *Jonsson* renders claim 5 obvious.

c. Claim element [5.5]

92. Claim element [5.5] recites “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.” The claim requires that the “password” is created based on “a token and a passcode,” where “the token” is “not known to the user.” *Compare* claim element [5.5] *with* claim element [5.3]. Petitioner argues that “*Veneklase*, alone or in combination with *Jonsson*, teaches this limitation.” Pet., p. 38 (emphasis added). I disagree.

93. As a threshold matter, *Veneklase* alone does not teach this limitation because *Veneklase* fails to disclose a “password” that is created based on “a token and a passcode,” as conceded by Petitioner. *See* Pet., p. 28 (*Veneklase* “does not disclose creating a new password based on those two items.”).

94. Further, Petitioner mapped *Veneklase*'s "code compare module 416" to the claimed "authentication module." See Pet., p. 38. *Veneklase* discloses "user 404 now enters the code he or she has received from the pager 420" and sends this "code back to computer 402 where it is compared within the software subroutine module denoted as 'code compare' 416." Ex. 1006, 8:18-27 (emphasis added). As discussed above in reference to claim element [5.3], Petitioner proposes modifying *Veneklase* with the teachings of *Jonsson* to meet the requirements of claim 5. *Jonsson* discloses an authentication process. See Ex. 1006, 9:1. "When the personal unit 20 receives an authentication challenge code, it prompts the user to input a PIN . . . and generates a response code by an algorithm having the challenge code . . . and the PIN." Ex. 1006, 9:9-13 (emphasis added). That response code is then "displayed on a display unit [of personal unit 20] for manual input to [user's] terminal," and then transmitted from the user's terminal to the system for comparison with an expected response code. *Id.*, 9:26-35.

95. In my opinion, Petitioner ignores the fact that the proposed combination requires modifying *Veneklase*'s "pager 420" to execute an algorithm that "calculates a response code based on the received challenge code [and] the user input (e.g., PIN)," as performed by *Jonsson*'s "personal unit 20." Ex. 1006, 8:12-14. First, in my opinion, Petitioner presents zero evidence that *Veneklase*'s "pager 420" is capable of executing such an algorithm. Further, *Veneklase* discloses its "invention

is very cost effective as it employs substantially ‘off the shelf’ and readily available components.” Ex. 1005, 22-24. But in my opinion, Petitioner provides zero evidence that an off-the-shelf pager, in 1996, was capable of executing specialized security algorithms. In fact, *Jonsson* expressly states that its algorithm requires a highly specialized “personal unit,” not just an off-the-shelf pager. See Ex. 1006, 6:24-7:23, Fig. 2. *Jonsson* even discloses that it is preferable that “the personal unit is a separate unit, thereby minimizing or avoiding the need to customize a [personal] communication device,” which teaches away from the Petitioner’s proposed combination. See *id.* at 7:24-26 (emphasis added).

96. It is my understanding that the Board rejected this argument in the Institution Decision:

We disagree with Patent Owner’s arguments. *Jonsson* explicitly teaches that “the capacity for performing the necessary calculations exists in conventional cellular telephones and personal communication units [(i.e. pagers)], allowing the present invention to be implemented through software.” Ex. 1006, 7:27–31. Thus, *Jonsson*’s disclosure provides evidence that pagers, such as Veneklasé’s pager 420, are capable of executing *Jonsson*’s algorithm.

Paper 9, p. 22. But in my opinion, the Board’s citation to *Jonsson* is incomplete. See *id.* (citing Ex. 1006, 7:27-31). The preceding sentence makes it clear that implementing the algorithm in a personal communication device requires

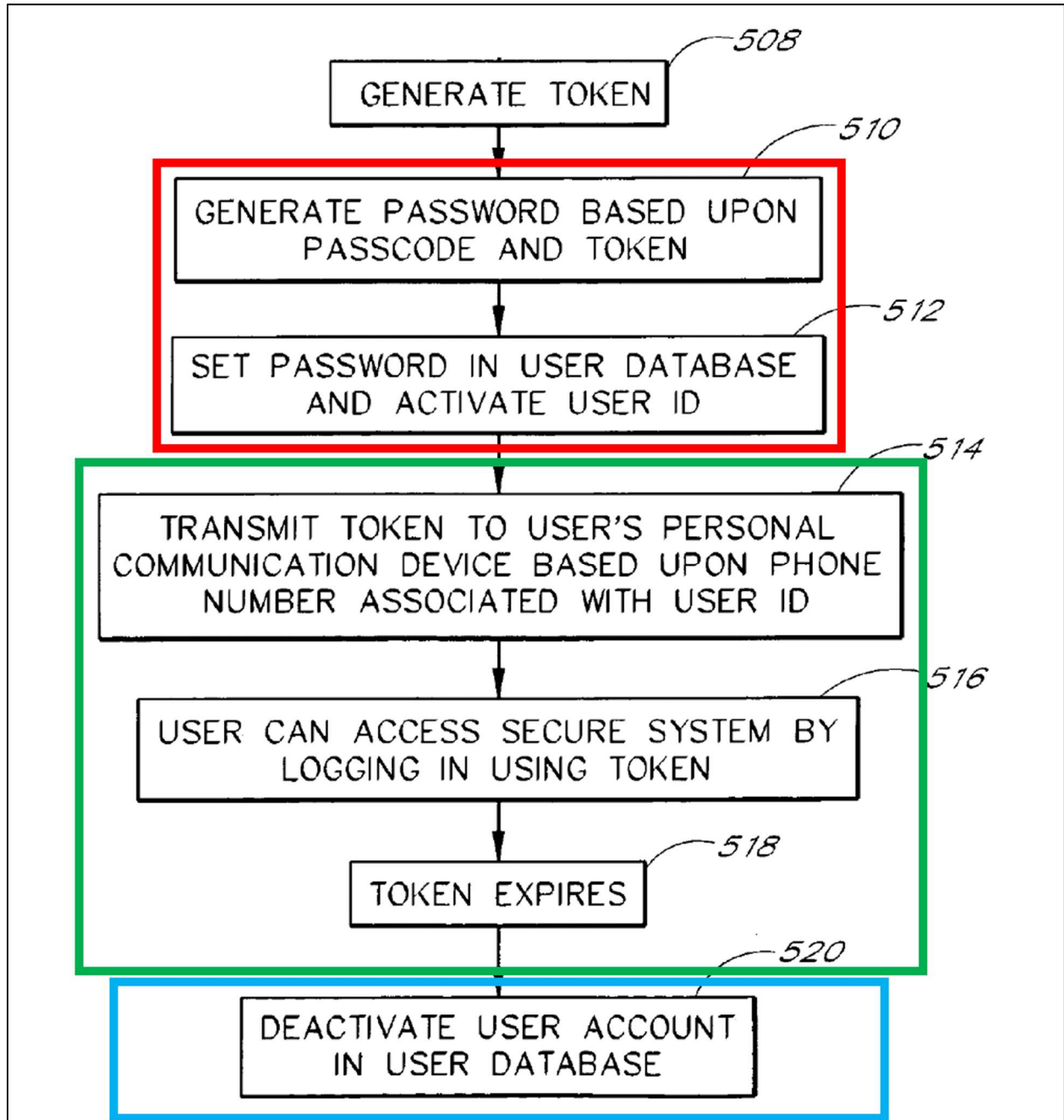
customization of that device: “In a preferred embodiment, the personal unit is a separate unit, thereby minimizing or avoiding the need to customize a communication device such as a cellular telephone.” *See* Ex. 1006, 7:24-26. Only by having that separate unit are the remaining devices in a cellular phone capable of performing the remaining tasks. *See id.* at 7:27-31. Accordingly, in my opinion, there is zero evidence in the record that *Veneklase*’s “pager 420” is capable of executing such an algorithm. To the contrary, in my opinion, the evidence indicates that *Veneklase*’s “pager 420” is not capable of executing such an algorithm.

97. In view of the above, in my opinion, Petitioner fails to show that the combination of *Veneklase* and *Jonsson* teaches or suggests claim element [5.5], and thus fails to show that the combination of *Veneklase* and *Jonsson* renders claim 5 obvious.

d. Claim element [5.6]

98. Claim element [5.6] recites “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.” Ex. 1001, 12:40-47 (emphasis added). It is my understanding that claim 5 requires activation of account access in response to generation of the claimed “new password.” I agree.

In my opinion, the language of the claim is clear: the “predetermined period of time” starts “after activating the account” and ends upon “deactivat[ion] [of] the account.” *See id.* The same process is depicted, for example, in Figure 5, which is reproduced in pertinent part below:



Ex. 1001, Fig. 5 (excerpted and annotated). Activating account access in response to generation of the new “password” is depicted in steps 510 and 512 of Figure 5 (as highlighted in red in Figure 5). *See id.* at 9:28-43, Fig. 5. Deactivation the account occurs in step 512 (as highlighted in blue in Figure 5). *See id.* at 9:61-64, Fig. 5. The “predetermined period of time” is the time period between those two events (as highlighted in green in Figure 5). *See id.* at 12:41-47, Fig. 5. In my opinion, Petitioner’s arguments fail for the following reasons.

99. First, Petitioner argues that *Veneklas* discloses account activation when code compare module 416 “allows access if the random codes match.” *See* Pet. at 41. That process occurs after code compare module 416 receives the random codes back from the user, unlike claim 5, which requires that the “authentication module” activates access to the account in response to creation of the new “password,” not in response to receiving the “password” from the user, after the token is sent to the user. *See Ex. 1005*, 8:1-26. That comparison step in is similar to step 516 in Figure 5 of the ’684 Patent, which occurs after activation of access, and after the “predetermined period of time” has begun (as highlighted in green above). In the ’658 Patent, the “authentication module” authenticates the user (i.e., permits access) by comparing the “password” received from the user with the “password associated with the user.” *See Ex. 1001*, 7:15-17 (“the authentication module 112 then compares hashes of passwords rather than the passwords

themselves to authenticate the user 108”), 9:54-59 (“The user then logs in using his user ID 152 and the password 158.”), Fig. 5. Thus, in my opinion, the Petition incorrectly identifies a process that occurs after compare module 416 receives the alleged “password” from the user, unlike claim 5, which requires that the “authentication module” activates access to the account in response to creation of the new “password,” not in response to receiving the “password” from the user.

100. Second, Petitioner argues that “the predetermined period would be the time between receipt of the token (e.g., randomly generated challenge code) and the sending back of the newly created password (e.g., response code).” Pet., p. 43. In my opinion, Petitioner’s argument is flawed on its face because the claimed “predetermined amount of time” is the timeframe between activation and deactivation of the account. See Ex. 1001, claim 5 (“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”). Petitioner’s argument rests on activation being “receipt of the token,” without any corresponding evidence that access to the account is activated upon receipt of the token. See Pet., pp. 41-46.

101. Third, in my opinion, even if Petitioner were correct, that configuration would be contrary to the claim language, which requires that the “authentication module” activate and deactivate access to the account. Ex. 1001, 12:37-47. The

Petition identifies “code compare module 416” in *Veneklase* as the alleged “authentication module,” which is part of the “host computer.” *See* Ex. 1006, Fig. 6. But Petitioner identifies a separate device, “pager 420,” as the “personal communication device” that receives the “token.” *See* Pet., p. 22 (“personal communication device (e.g., pager 420)”); Ex. 1001, 12:34-26. Because the Petition alleges that the “predetermined period of time” begins with “receipt of the token (e.g., randomly generated challenge code)” by “pager 420,” it would be the “personal communication device,” not the “authentication module” (i.e., “code compare module 416” in the “host computer”) that activates access to the account. *See* Pet., p. 43.

102. Fourth, Petitioner argues that “the predetermined period would be the time between receipt of the token (e.g., randomly generated challenge code) and the sending back of the newly created password (e.g., response code).” Pet., p. 43 (emphasis added). In other words, under Petitioner’s theory, the duration of the “predetermined period of time” varies by when the user decides to send back the response code. *See id.* If the user decides to send back to the response code immediately, the alleged “predetermined period of time” would be short, possibly on the order of seconds. *See id.* If, instead, the user waits five minutes before sending, the alleged “predetermined period of time” would be on the order of five minutes. *See id.* Thus, in my opinion, the period of time identified in the Petition is

not predetermined; rather, it is driven by the user's activity, which is contrary to the plain language of this claim element.

103. Because the Petition fails to show that the asserted combination activates access to the account in response to the password, the Petition also fails to show that the asserted combination deactivates the account within a predetermined amount of time after activating the account.

104. In view of the above, in my opinion, the combination of Veneklase and Jonsson fails to teach or suggest claim element [5.6], and thus fails to render claim 5 obvious.

B. Ground 2 – *Kew* and *Sormunen* Do Not Render Claims 1 and 3-6 Obvious

105. In my opinion, *Kew* and *Sormunen* (the “Ground 2 References”) do not render obvious any of claims 1 and 3-6.

1. Independent Claim 5

106. In my opinion, the Ground 2 References do not render obvious independent claim 5 at least because they does not teach or suggest the following elements of independent claim 5.

a. Claim element [5.3]

107. Claim element [5.3] 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.” ’658 Patent, claim 5 (emphasis added). Petitioner argues that this limitation is met by the “security server” in *Kew*. Pet., p. 60. Petitioner does not argue that it would have been obvious to modify the asserted prior-art combination to meet this limitation. *See* Pet., pp. 60-64.

108. In my opinion, on its face, the Petition does not teach or suggest this limitation because it fails to even consistently identify the alleged “passcode” for in *Kew*:

Thus, *Kew* teaches *a control module executed on the computer processor (e.g., a portion of security server 5) configured to create a new password (e.g., transformed code (Code B)) based at least upon a token (e.g., random code (Code A)) and a passcode (e.g., identity code), wherein the token is not known to the user (e.g., random code generated by server) and wherein the passcode is known to the user (e.g., his actual name or PIN), the control module further configured to set a password associated with the user to be the new password (e.g., using transformed code (Code B) as the new password).* EX1003, ¶¶136-140.

109. Pet., pp. 62-63. In one instance, Petitioner identifies *Kew*’s “identity code” as the claimed “passcode,” and in another instance, Petitioner identifies the “actual name or PIN” as the claimed “passcode.” *See id.* But neither is the claimed “passcode.”

110. In my opinion, *Kew's* “identity code” is not the claimed “passcode” because this claim element requires that “the passcode is known to the user.” *Kew's* “identity code is a key for the one-way algorithm and is such that when applied to the algorithm, together with a code to be encrypted the resultant code is characteristic of the particular receiver unit 6.” Ex. 1007, 7:29-32 (emphasis added). The “identity code” is stored in the EPROM of receiver unit 6. Ex. 1007, 7:28-39. It is important to note that “[t]he receiver unit 6 therefore uses the received random number and the identity code stored in its own EPROM to produce a transformed code (Code C) via its own characteristic algorithm,” not the user. See Ex. 1007, 8:33-36 (emphasis added). That is why *Kew* contains no disclosure of the user knowing the “identity code.”

111. Moreover, in my opinion, a POSITA would understand that the “identity code” would not be known to the user, as is required by the claim. For example, the “identity code” is stored in the EPROM of receiver unit 6. EPROM (erasable programmable read-only memory) is a type of non-volatile memory. Ex. 2005, p. 195. They are “reprogrammed by removing the protective cover from the top of the chip and exposing the chip to ultraviolet light.” Ex. 2005, p. 195. I have experience in using such chips. Specifically, you use the UV to erase them and then subsequently reprogram them with a EPROM programming device like that pictured here:



<http://www.advin.com/eprom-programmer.htm>. As one can see this is not a simple process available to any average computer user. In my opinion, the choice in *Kew* to store the “identity code” in EPROM, as opposed to RAM (that would give utility to knowing the identity code), indicates to a POSITA that the “identity code” is not input to receiver unit 6 by the user; rather the device is pre-programmed with the “identity code.” In my opinion, a POSITA would generally understand that such programming of such codes would be generated at the server side and then pre-programmed onto the device. In such case the user’s knowledge of the “identity code” is not required. That is why a POSITA, in my opinion, would understand that the “identity code” would not need to be known to the user, as is required by this claim element.

112. In my opinion, the Petition confuses the “identity code” and the “user identification code:”

The identity “code may take any suitable form, for example his actual name or preferably a more secure code such as a PIN.” EX1007, 7:36-8:2. A POSITA would have understood that PINs that are “treated by the user as a secret code” are known to the user in order for them to be treated as such.

See Pet., p. 62. But *Kew* discloses the following:

When the user seeks access to the host system 1 via the terminal 2, he enters his user identification code. This code may take any suitable form, for example his actual name or preferably a more secure code such as a PIN.

Ex. 1007, 7:36-8:2 (emphasis added). In my opinion, the “identity code” and the “user identification code” are not the same thing. Compare Ex. 1007, 7:29-30 with Ex. 1007, 2:28-30. The “identity code is a key for the one-way algorithm” (Ex. 1007, 7:29-30), whereas the “user identification code” is used to identify the user, like a username. See Ex. 1007, 2:28-30 (“When the user enters his user identification code, the host computer system identifies the corresponding transformation algorithm in a database. . . .”); see also Ex. 1007, 11:8-11. Thus, in my opinion, Petitioner’s mischaracterization of the “identity code” is not correct.

113. *Kew*'s "actual name or PIN" are not the claimed "passcode" because neither is part of the claimed "password," along with the claimed "token," as is required by this claim element. *See* Ex. 1001, 12:28-30. As the Petition concedes, "*Kew* discloses that the security server creates a new password (e.g., transformed code (Code B)) based on a token (e.g., random code (Code A)) and a passcode (e.g., identity code) via an encryption mechanism." *See* Pet., p. 60 (emphasis added); *see also* Ex. 1007, 7:28-8:10, 8:33-36, 11:6-15, Fig. 2. In my opinion, the "actual name or PIN" are used to identify the user's "identity code," like a username, not as part of a password. *See* Ex. 1007, 7:34-8:5. This is further supported by Petitioner's concession that alleged "password" received from the user in claim element [5.5] is the combination of "the received random number and the identity code," not the user's "actual name or PIN." *See* Pet., p. 64.

114. *Kew* also fails to disclose the claimed "token." This claim element requires that "the token is not known to the user." Ex. 1001, 12:29-30. Petitioner contends "[not known to the user] must mean 'not known to the user before being sent to the user as part of the authentication process' . . . a POSITA would have understood that the token would eventually need to be known to the user." Petition, p. 10 (emphasis added). And Petitioner contends that "random code (Code A)" disclosed in *Kew* is the claimed "token." Pet., p. 60. But the Petition provides zero evidence that *Kew*'s "Code A" is "eventually . . . known to the user." *See id.* at 60-

63. Rather, *Kew* discloses that “Code A” (Petitioner-identified “token”) is transmitted to a receiver held by the user, the receiver transforms “Code A” to “Code C,” and the receiver has a means for displaying “Code C.” *See* Ex. 1007, 2:14-19, 4:6-7 (“The means for displaying Code C on the receiver can be a liquid crystal display.”). But *Kew*’s “Code A” (Petitioner-identified “token”) is never displayed to the user, and thus “Code A” is not “eventually . . . known to the user,” as Petitioner argues. There is no need to display “Code A” to the user because the receiver transforms “Code A” to “Code C,” not the user. *See id.* at 2:14-19.

115. For at least these reasons, in my opinion, *Kew* fails to teach or suggest claim element [5.3]. *Sormunen* does not cure the deficiencies of *Kew*, and the Petition does not so allege. *See* Pet., pp. 60-63. Accordingly, in my opinion, the combination of *Kew* and *Sormunen* does not teach or suggest this claim element.

b. Claim element [5.6]

116. Claim element [5.6] recites “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.” ’658 Patent, 12:40-47 (emphasis added). The “password” in this claim element is set (from the “new password”) by the “control module” and is “based at least upon a token and a

passcode.” *Compare* claim element [5.6] *with* claim element [5.3]. Thus, creation of “password” by the “control module” (which requires creation of the token), is what causes the “authentication module” to activate access to the account: “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. . . .” ’658 Patent, 12:40-43 (emphasis added). That process is depicted, for example, in Figure 5, which shows that the password is generated (step 510), the account is activated when the password is set in the user database (step 512), then the token is transmitted to the user’s personal communication device (step 514):

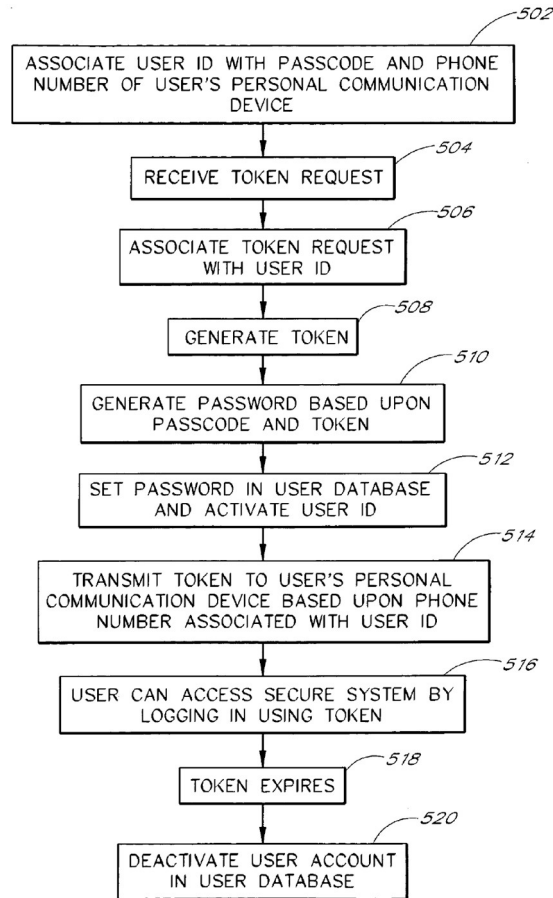


FIG. 5

'658 Patent, Fig. 5. Only then can the user access the secure system (step 516), before the token expires (step 518), at which point access to the account is deactivated (step 520). *See id.*

117. In my opinion, the Petition fails to show that *Kew* discloses activating account access in response to generation of the new “password,” which is “based at least upon a token and a passcode.” *See Pet*, pp. 67-72. The Petition alleges that the security server in *Kew* comparing the stored password with the password received from the user “activates access to the account in response to the password:”

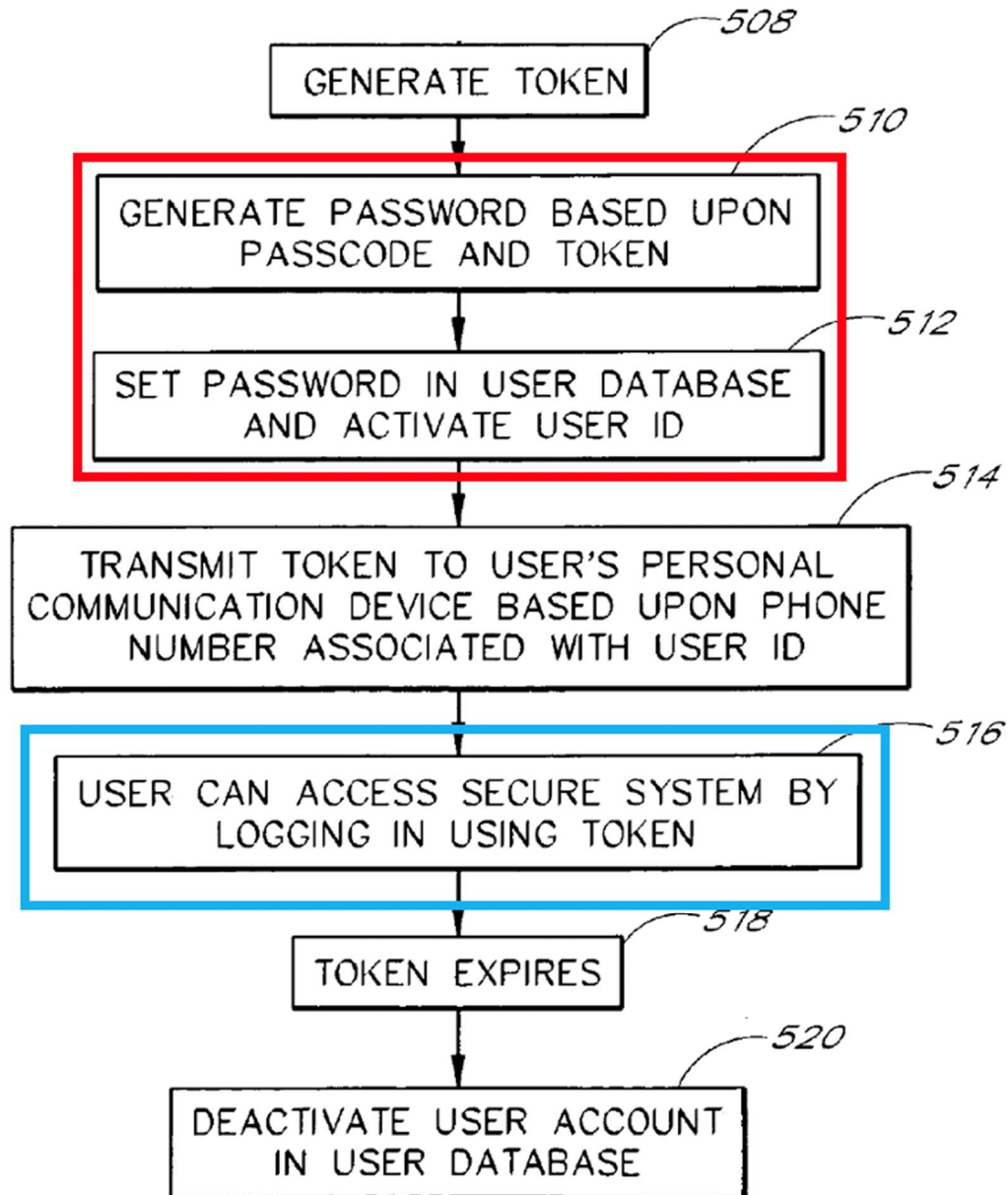
Kew discloses wherein the authentication module (e.g., a portion of security server 5) activates access to the account in response to the password (e.g., if Code B and Code C are identical, access to the host system 1 is permitted). Specifically, *Kew* discloses that once the user has input the transformed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

Pet., p. 67 (emphasis added). More specifically, “security server 5” generates “code B,” whereas the user’s “receiver unit 6” generates “code C.” *See* Ex. 1007, 8:5-10, 8:33-36. The user then inputs “code C” so that “security server 5” can compare “code B” with “code C” to determine if they match:

The terminal 2, at the behest of the security server 5 prompts the user to input the transformed Code C displayed by the receiver unit 6. After input, the security server 5 compares the input Code C with the transformed code, Code B, it produced by encryption of the random code, Code A. If Code B and Code C are identical, access to the host system 1 is permitted.

Ex. 1007, 9:5-11. Access to the system is permitted if “code C” and “code B” match. *See id.* Comparing a received password with the password stored on a server is a standard way of determining whether to permit access. But, in my opinion, that process is different than activating access to the account, as required by this claim

element. That difference is depicted in Figure 5, which is reproduced in pertinent part below:



'658 Patent, Fig. 5 (excerpted and annotated). This claim element requires activating account access in response to generation of the new "password," which is depicted in steps 510 and 512 of Figure 5 (as highlighted in red in Figure 5). See '658 Patent

at 9:28-43, Fig. 5. And that process occurs before the “token” is transmitted to the user in step 514. *See id.*

118. The comparison step in *Kew* that the Petition contends discloses this claim element is markedly different. That step necessarily occurs after the “token” is transmitted to the user because “code C” is generated by “receiver unit 6,” in part based on the “identity code” that Petitioner contends is the claimed “token.” *See* Ex. 1007, 7:28-32, 8:33-36; Pet., p. 60 (“token (e.g., random code (Code A))”). Moreover, in my opinion, the comparison step in *Kew* is akin to step 516 in Figure 5 of the ’684 Patent (as highlighted in blue). In the ’658 Patent, the “authentication module” authenticates the user (i.e., permits access) by comparing the “password” received from the user with the “password associated with the user.” *See* ’658 Patent at 7:15-17 (“the authentication module 112 then compares hashes of passwords rather than the passwords themselves to authenticate the user 108”), 9:54-59 (“The user then logs in using his user ID 152 and the password 158.”), Fig. 5. Thus, the Petition incorrectly identifies a process that occurs after security server 5 receives the alleged “password” from the user, unlike claim 5, which requires that the “authentication module” activates access to the account in response to creation of the new “password,” not in response to receiving the “password” from the user. *See* Ex. 1005, 8:1-26.

119. Claim element [5.6] recites “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.” ’658 Patent, 12:40-47 (emphasis added). The Petition identifies “a portion of security server 5” as the alleged “authentication module.” *See* Pet., p. 64. But does not identify any disclosure about that security server deactivating access to the account. *See id.*, pp. 66-71. Instead, the citations identified in the Petition relate solely to receiver unit 6, which the Petition alleges is the “personal communication device.” *See id.* (citing Ex. 1007, 3:14-17, 3:19-23; 8:33-9:3); *see also* Pet., p. 53 (“the receiver unit 6 can be a personal communication device, such as a pager”). The first citation states that “the receiver can only be enabled for a predetermined period. . . .” Ex. 1007, 3:14-17 (emphasis added). The second citation states that the receiver will not allow an authorized user to use it after a predetermined period. *See id.*, 3:19-23. The third citation states that the receiver will only display a code to the user for a predetermined period of time. *See id.*, 8:33-9:3. Again, the Petition does not identify any disclosure of “security server 5” deactivating access to the account after a predetermined amount of time in *Kew*. That is because, in my opinion, *Kew* contains no such disclosure. To the contrary, the disclosure of *Kew* indicates that account

access remains active indefinitely after “Code A” has been transmitted. *See* Ex. 1007, 8:11-9:11, 12:6-13:6. In my opinion, the disclosures cited by Petitioner merely indicate that the screen of receiver unit 6 can be locked/unlocked through the use of “a second user identification code,” which is much like the standard security features on a mobile phone. *See* Ex. 1007, 8:25-29. In my opinion, the “predetermined length of time” relied upon in the Petition does nothing more than lock the screen after a predetermined length of time, at which point it can be unlocked again. *See* Ex. 1007, 8:25-9:3. But there is no disclosure to indicate that security server 5 deactivates access to the account when the screen of receiver unit 6 is locked. Nor could there be because receiver unit 6 is described as a receive-only device that receives information through a pager network. *See* Ex. 1007, 1:31-32, 2:14-19, 3:14-17, 3:31-35, 4:8-12, 8:11-23, 8:29-36. Thus, there would be no mechanism for receiver unit 6 to signal security server 5 to deactivate access to the account in response to expiration of the “predetermined length of time” on receiver unit 6.

120. For these reasons, it is my opinion that *Kew* fails to teach or suggest claim element [5.6]. *Sormunen* does not cure the deficiencies of *Kew*, and the Petition does not so allege. *See* Pet., pp. 66-71. Accordingly, it is my opinion that the combination of *Kew* and *Sormunen* does not render independent claim 5 obvious.

2. Dependent Claim 6

121. Dependent claim 6 depends from and adds limitations to independent claim 5. In my opinion, the combination of *Kew* and *Sormunen* fails to render obvious claim 5 unpatentable, therefore, the combination of *Kew* and *Sormunen* fails to render obvious dependent claim 6 for at least the same reasons.

3. Independent claim 1

122. In my opinion, the combination of *Kew* and *Sormunen* does not render obvious independent claim 1 because the combination does not teach or suggest the following elements of the claim.

123. Petitioner argues that “[m]ost limitations of claim 1 are substantively similar to claim 5. Therefore, these limitations are obvious for the same reasons as the corresponding limitations in claim 5.” Pet., pp. 72-73. As discussed above, in my opinion, the combination of *Kew* and *Sormunen* fails to teach or suggest claim elements [5.3] and [5.6]. Accordingly, the combination also fails to teach or suggest the corresponding limitations in independent claim 1. Thus, in my opinion, the combination does not render independent claim 1 obvious.

a. Claim element [1.2]

124. In my opinion, the combination of *Kew* and *Sormunen* does not render independent claim 1 obvious for the additional reason that the combination fails to teach or suggest claim element [1.2]. Claim element [1.2] recites “receiving a

request from the user for a token via the personal communication device, over the second network,” wherein the “second network is a cell phone network.” *Compare* claim element [1.2] *with* claim element [1.1] (“wherein said second network is a cell phone network”). Petitioner mapped *Kew*’s “receiver unit 6” and “Code A” to the claimed “personal communication device” and claimed “token,” respectively. *See* Pet., pp. 56, 60, 73, 74. In my opinion, *Kew* alone, however, does not disclose this claim element. *See* Pet., p. 74 (“*Kew*, in combination with *Sormunen*, teaches this limitation”). That is because *Kew* expressly discloses that the request comes from “terminal 2,” which is a different device than the alleged “personal communication device” identified by Petitioner (i.e., “receiver unit 6”). *See* Pet., p. 53 (“receiver unit 6 can be a personal communication device, such a pager”); *see also* Ex. 1007, 7:34-8:10. Accordingly, in my opinion, Petitioner’s proposed combination of *Kew* and *Sormunen* fails to support a conclusion of obviousness for multiple reasons.

125. *Kew* discloses a system that (a) receives a “user identification code” of a user from a “terminal” when the user seeks access to the system, (b) transmits a code (“Code A”) to the “receiver unit” corresponding to the user, (c) receives a new code (“Code C”) from the terminal, where “Code C” is calculated by and displayed on the “receiver unit” for the user, and (d) grants the user access to the system if received “Code C” matches a code (“Code B”) internally calculated by the system. *See* Ex. 1007, 2:25-36, 7:34-9:11. Accordingly, in my opinion, this sequence of

events is fundamental to *Kew*'s authentication process and thus is a key/core feature of *Kew*'s principle of operation.

126. Petitioner's proposed modification to *Kew* includes having *Kew*'s "receiver unit" (Petitioner-identified "personal communication device") transmit a request for *Kew*'s "Code A" (Petitioner-identified "token") to *Kew*'s system, as taught by *Sormunen*'s "paging terminal 3" transmitting "a password request." See Pet., pp. 74-75 (citing Ex. 1008, 5:35-38, 6:20-24, Fig. 2). But *Kew* never discloses that the "receiver unit" is capable of any transmission, let alone transmission on "a cell phone network" (see Ex. 1007, 7:20-8:24), and Petitioner provides no evidence of transmission capabilities. See Pet., pp. 74-75. Nor does Petitioner provide any evidence regarding modification to include transmission capabilities. See *id.* Thus, in my opinion, the proposed modification has no reasonable expectation of success.

127. Further, Petitioner's proposed modification changes the fundamental sequence of events in *Kew*'s authentication process. In my opinion, this violates *Kew*'s principle of operation. Accordingly, the proposed modification of *Kew* is far too drastic to be considered obvious, and thus the combination of *Kew* and *Sormunen* fails to render claim 1 obvious.

128. Additionally, or alternatively, the system in *Kew* transmits "Code A" (Petitioner-identified "token") in response to receiving *Kew*'s "user identification code." Ex. 1007, 7:34-8:24. Thus, *Kew*'s "receiver unit" (Petitioner-identified

“personal communication device”) would necessarily need to include *Kew*’s “user identification code” in its request for *Kew*’s “Code A” (Petitioner-identified “token”).

129. But *Kew* also requires that the “user identification code” be transmitted to *Kew*’s system via *Kew*’s “terminal.” See Ex. 1007, 7:34-35, 8:25-26. At a minimum, this must be done to identify the “terminal” where the user is located and thus identify the “terminal” where the user should be “prompt[ed] . . . to input the transformed Code C displayed by the receiver unit 6.” Ex. 1007, 7:10-18, 9:5-7, Fig. 1 (showing multiple terminals). Accordingly, Petitioner’s proposed combination requires transmitting *Kew*’s “user identification code” twice, on two separate devices, for a single session with *Kew*’s system.

130. *Kew* discloses the “user identification code” is “preferably a more secure code such as a PIN.” Ex. 1007, 8:1-2. In my opinion, increasing the number of times the “user identification code” is transmitted only increases the likelihood of it being intercepted. Accordingly, in my opinion, this double transmission of *Kew*’s “user identification code” with no ascertainable benefit is not rational. Thus, Petitioner’s proposed modification does not render claim 1 obvious.

131. For these reasons, in my opinion, the combination of *Kew* and *Sormunen* does not render claim 1 obvious.

4. Dependent Claims 3 and 4

132. Dependent claims 3 and 4 depend from and add limitations to independent claim 1. In my opinion, the combination of *Kew* and *Sormunen* fails to render obvious claim 1 unpatentable, therefore, the combination of *Kew* and *Sormunen* fails to render obvious dependent claims 3 and 4 for at least the same reasons.

VI. CONCLUSION

133. For the foregoing reasons, it is my opinion that the Challenged Claims of the '658 Patent are patentable.

134. I reserve the right to modify and/or supplement this declaration, to present further analysis, and/or to amend my opinions as more and/or other arguments and/or information becomes available.

135. I hereby declare that all statements made herein of my knowledge are true and that all statements made on information and belief are believed to be true. The statements in this declaration were made with the knowledge that willful false statements and the like are made punishable by fine or imprisonment under Section 1001 of Title 18 of the United States Code and may jeopardize the validity of the application or any patent issuing thereon.



Date: October 10, 2023

Rajeev Surati