

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, LLC,

Petitioner,

v.

DYNAPASS IP HOLDINGS, LLC

Patent Owner.

***Inter Partes* Review No. IPR2023-00425**

Patent No. 6,993,658

**PATENT OWNER'S RESPONSE TO THE PETITION
FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 6,993,658**

Filed on behalf of Patent Owner by:

John Wittenzellner (Reg. No. 61,662)
1735 Market Street, Suite 125, #453
Philadelphia, PA 19103

Todd E. Landis (Reg. No. 44,200)
2633 McKinney Ave., Suite 130
Dallas, TX 75204

Mark McCarthy (Reg. No. 69,575)
601 Congress Ave., Suite 600
Austin, TX 78701

WILLIAMS SIMONS & LANDIS PLLC

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	PETITIONER’S ASSERTED GROUNDS OF UNPATENTABILITY	1
III.	THE ’658 PATENT	1
IV.	CLAIM CONSTRUCTION	9
V.	RESPONSE TO ISSUES RAISED IN THE PETITION AND THE INSTITUTION DECISION	12
A.	Ground 1 – The Combination of Veneklas and Jonsson Does Not Render Obvious Claim 5 of the ’658 Patent.....	12
1.	Independent Claim 5	16
i.	[5.3] “a control module . . . configured to create a new password based at least upon a token and a passcode”.....	16
ii.	[5.4] “a communication module configured to transmit the token to the personal communication device through the cell phone network”	23
iii.	[5.5] “an authentication module configured to receive the password from the user through a secure computer network”	28
iv.	[5.6] “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”	32
B.	Ground 2 – The Combination of Kew and Sormunen Does Not Render Obvious Claims 1 and 3-6 of the ’658 Patent.....	38
1.	Independent Claim 1	41
i.	[5.3] “a control module . . . 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”	42

ii.	[5.6] “wherein the authentication module . . . deactivates the account within a predetermined amount of time after activating the account”	47
2.	Dependent Claim 6.....	41
3.	Independent Claim 1	55
i.	[1.2] “receiving a request from the user for a token via the personal communication device, over the second network”	55
4.	Dependent Claims 3 and 4	59
VI.	THE BOARD DOES NOT HAVE JURISDICTION OVER EXPIRED PATENTS.....	60
VII.	CONCLUSION.....	61

TABLE OF AUTHORITIES

Cases

<i>In re Ratti</i> , 270 F.2d 810 (CCPA 1959).....	19, 58
<i>Intelligent Bio-Systems, Inc. v. Illumina Cambridge, Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016).....	57
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007)	59
<i>McGinley v. Franklin Sports, Inc.</i> , 262 F.3d 1339 (Fed. Cir. 2001).....	26
<i>Oil States Energy Servs., LLC v. Greene’s Energy Grp., LLC</i> , 138 S. Ct. 1365 (2018)	60
<i>Plas-Pak Indus. v. Sulzer Mixpac AG</i> , 600 F. App’x. 755 (Fed. Cir. 2015).....	19, 58

Other Authorities

MPEP § 2143.01	19, 58
----------------------	--------

EXHIBIT LIST

Exhibit	Description
2001	Google Patents webpage for U.S. Patent No. 6,993,658, https://patents.google.com/patent/US6993658B1/
2002	“Preliminary Constructions,” <i>Dynapass IP Holdings, LLC v. JPMorgan Chase & Co., et al.</i> , No. 2:22-cv-00212-JRG-RSP (E.D. Tex.)
2003	Declaration of Rajeev Surati
2004	CV of Rajeev Surati
2005	Microsoft Computer Dictionary (5th ed. 2002)

I. INTRODUCTION

Dynapass IP Holdings, LLC (“Patent Owner”) respectfully submits this Response (the “Response”) to the Petition for *Inter Partes* Review of U.S. Patent No. 6,993,658 (IPR2023-00425, the “Petition”) filed by Unified Patents, LLC (“Petitioner”). Petitioner fails to show unpatentability of claims 1 and 3-6 of the ’658 Patent (the “Challenged Claim(s)”) because Petitioner’s Grounds fail to disclose or render obvious one or more elements of each Challenged Claim. In addition, this proceeding should be terminated because the Board does not have jurisdiction over the expired ’658 Patent.

II. PETITIONER’S ASSERTED GROUNDS OF UNPATENTABILITY

Petitioner assert that claims 1 and 3-6 of the ’658 Patent are unpatentable under the following grounds:

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

Pet., p. 2.

III. THE ’658 PATENT

The ’658 Patent, which is titled “Use of Personal Communication Devices for User Authentication,” was filed on March 6, 2000, and issued on January 31, 2006.

Ex. 1001. The '658 Patent relates 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 at 1:7-11.

At the time of the claimed inventions, “secure systems”¹ used “a user ID and password pair to identify and authenticate system users.” *See id.* at 1:13-14. Although user ID/password pairs were ubiquitous, they suffered from several shortcomings, as recognized by the inventors of the '658 Patent:

Passwords created by users are often combinations of words and names, which are easy to remember but also easily guessed. Guessing passwords is a frequent technique used by “hackers” to break into systems. Therefore, 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. A user’s inability to remember complex combinations of letters, numbers, and symbols often results in the password being written down, sometimes on a note stuck to the side of a workstation.

Id. at 1:28-38.

¹ The '658 Patent describes many non-limiting examples of a “secure system,” including Novell NetWare-, Microsoft NT-, Windows 2000-, and UNIX/Linux-based computers, as well as “any system, device, account, “a user account on a network of computer workstations, a user account on a website, or a secure area of a building.” Ex. 1001 at 1:13-19, 4:13-23.

The increasing use of remote connectivity at the time of the claimed inventions further exacerbated the shortcomings of user ID/password pairs. *See id.* at 1:20-26. As a result, then-current systems faced several issues:

Present systems face several problems: users dread frequent password changes, frequent password changes with hard-to-remember passwords inevitably result in users surreptitiously writing down passwords, and security is compromised when users write down their passwords.

Id. at 1:39-43. Two-factor authentication (a form of multi-factor authentication) improves user ID/password pairs by adding “unpredictable, one-time-only access codes.” *See id.* at 1:49-51. The first factor is “a user passcode or personal identification number.” *See id.* at 1:46-47. The second factor is the “unpredictable, one-time-only access codes.” *See id.* at 1:49-51. In two-factor authentication, system access is based upon:

- “nonsecret information known to the user, such as the user ID;”
- secret information known to the user, such as the passcode;” and
- “information provided to the user through an object possessed by the user, such as the token.”

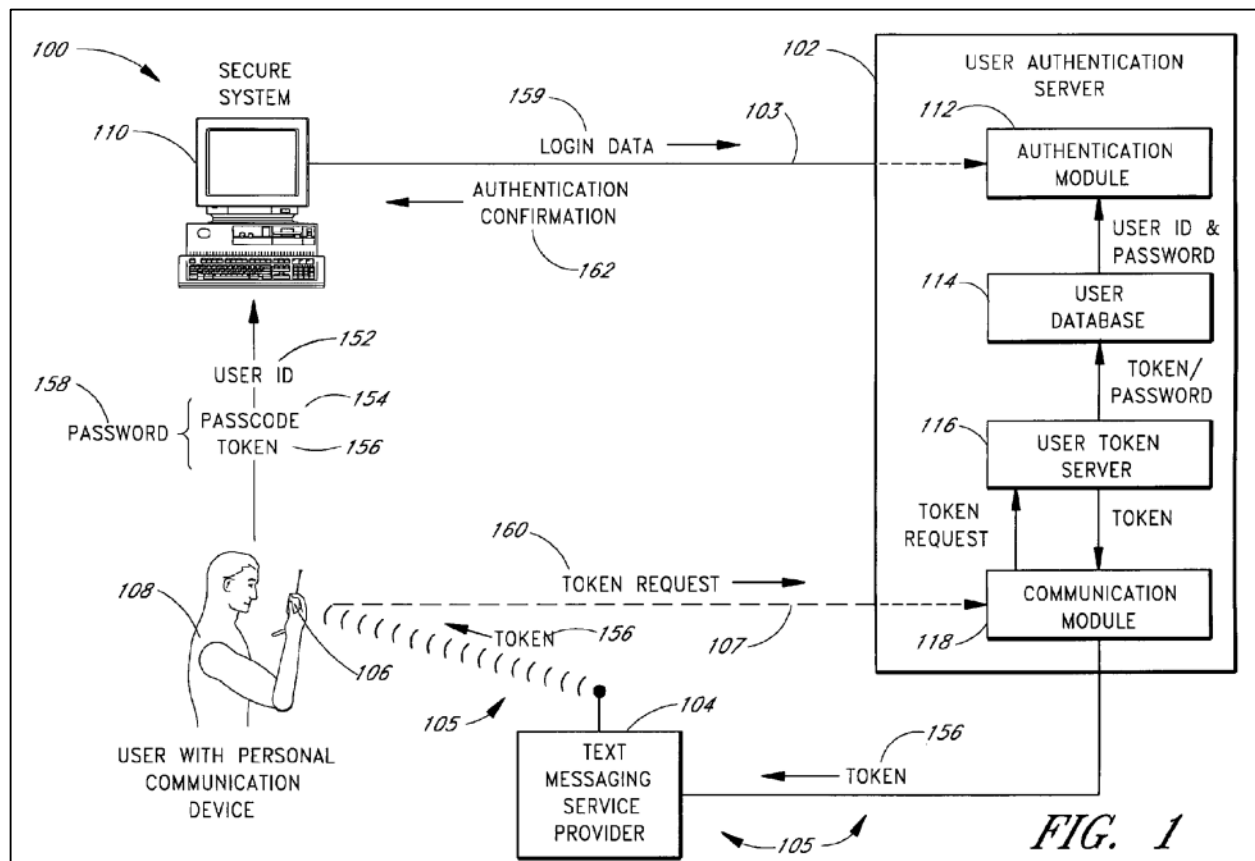
Id. at 2:11-15.

The '658 Patent acknowledges the existence of the RSA Security, Inc. SecurID product at the time of the claimed inventions, but identified significant deficiencies in the product:

The SecurID product, however, requires users to carry an additional item on their person in order to access a secure system. It would be advantageous if the benefits of the SecurID system could be achieved using a device that many users already carry—a personal communication device such as a mobile phone or a pager.

Id. at 1:54-59. The '658 Patent requires the use of a personal communication device, which teaches away from a separate device like the SecurID product. *See id.*

The '658 Patent solves the deficiencies of the SecurID product and further improves two-factor authentication in a unique, novel, non-obvious way. Figure 1 of the '658 Patent, reproduced below, depicts an embodiment of a user authentication system (identified as “100” in the figure):



Ex. 1001, at Fig. 1; *see also id.* at 3:31-33.

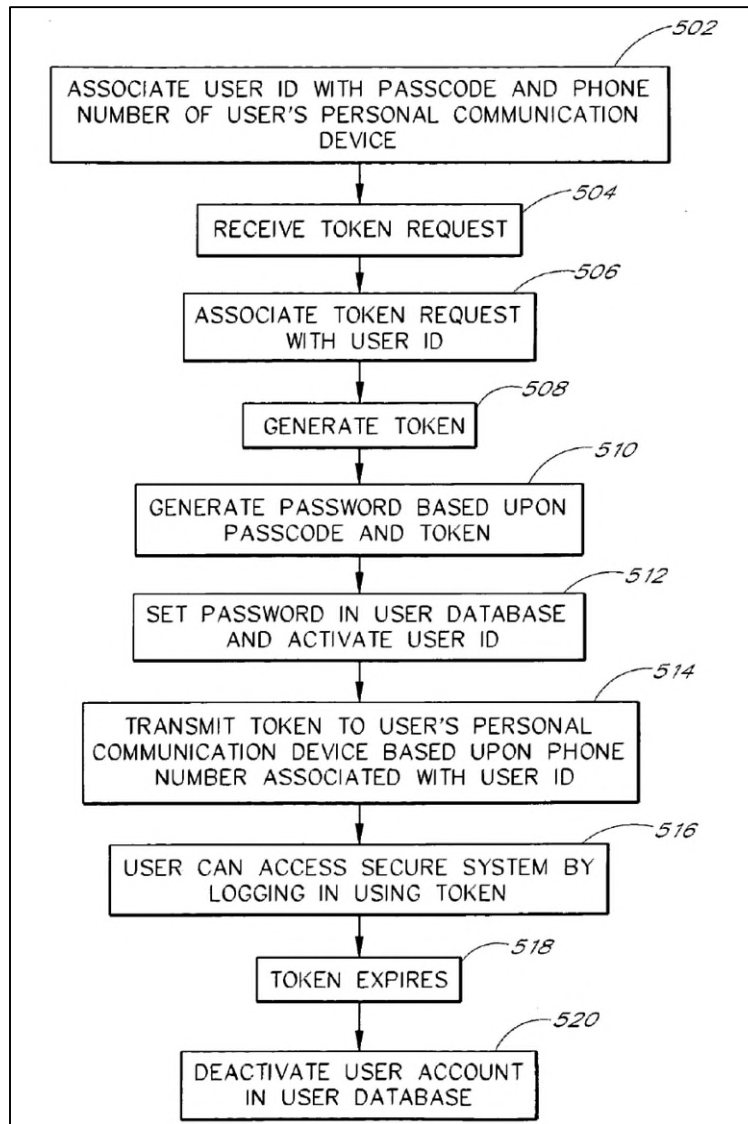
Authentication system (100) regulates access to secure system (110). *Id.* at 4:9-13. User authentication server (102) “preferably includes a program or a suite of programs running on a computer system to perform user authentication services.” *Id.* at 4:27-29. “The authentication information preferably includes a user ID 152, a passcode 154 and a user token 156.” *Id.* at 4:36-39. Tokens are received on the user’s personal communication device (106), which can be, for example, “a pager or mobile phone having SMS (short message service) receive capability.” *Id.* at 4:13-15.

It is important to be aware of the terminology used by the ’658 Patent. The “user ID may be publicly known and used to identify the user.” *Id.* at 4:39-40. The ’658 Patent uses the term “passcode” to refer to what is commonly called a “password.” “For example, the user 108 can combine a valid, memorized passcode of ‘abcd’” *Id.* 4:54-55; *see also id.* at 1:27-29 (“Passwords created by users are often combinations of words and names, which are easy to remember but also easily guessed.”), 4:40 (The passcode 154 is preferably secret and known only to the user 108.”). The “token” can be, for example, “a random or pseudo-random sequence of numbers or digits or both numbers and digits.” *Id.* at 9:22-24.

The ’658 Patent uses the term “password” to refer to the combination of at least the “passcode” and a “token.” *Id.* at 4:52-53 (“In the preferred embodiment,

the user 108 combines the token 156 with the passcode 154 to form a password 158.”). For example, if the passcode is “abcd” and the token is “1234,” the password could be “abcd1234” or “1234abcd.” *See id.* at 4:54-56. The components of the password (e.g., the passcode and token) can be combined or sent to the system as separate components. *See id.* at 4:52-65.

Figure 5, reproduced below, depicts an embodiment of how the system provides tokens and authenticates users.



Id. at Fig. 5; *see also id.* at 3:41-43.

In step 502, the system associates the user's user ID and passcode with the user's personal communication device. *Id.* at 8:53-60. By doing so, the system transmits the token only to the associated user. *See id.* In steps 504, 506, and 508, the system receives a request for a token, determines which user made the request (i.e., associates the request with a user ID), and generates the token. *See id.* at 9:3-

27, Fig. 5. Those steps differ from other systems that continually generate access codes. *See, e.g., id.* at 1:49-51 (“The SecurID card generates and displays unpredictable, one-time-only access codes that automatically change every 60 seconds.”). In step 510, the system generates a new “password” based on at least the “token” and “passcode.” *Id.* at 9:28-33, Fig. 5. That password is then stored and the user’s account can be activated if it was deactivated. *Id.* at 9:34-41, Fig. 5 (step 512).

In step 514, the system transmits the token to the user’s personal communication device. *See id.* at 9:44-53, Fig. 5. Claim 1 of the ’658 Patent requires that the “personal communication device” be “in communication over a second network, wherein said network is a cell phone network. . . .” *Id.* at 11:47-50. Claim 5 requires that the token is transmitted to the “personal communication device” through a “cell phone network.” *Id.* at 12:34-36. The claims also require that the user’s account is deactivated “within a predetermined amount of time” after the account is activated. *Id.* at 12:9-13 (claim 1), 12:41-47 (claim 5).

The Patent Office issued the ’658 Patent issued after several office actions. Since then, the ’658 Patent has been cited by more than 200 patent applications. Ex. 2001, <https://patents.google.com/patent/US6993658B1/>. Amongst those patent applications are patent applications filed by major industry entities, including IBM Corporation, Microsoft Corporation, Lucent Technologies, Honeywell International,

Inc., British Telecommunications PLC, AT&T, Visa, and Google Inc. *See id.* They also include a patent application filed by JPMorgan Chase Bank, N.A., a defendant in the parallel district court proceedings in the Eastern District of Texas. *See id.*

IV. CLAIM CONSTRUCTION

Patent Owner respectfully submits that the Board instituted *inter partes* proceedings based, in part, on an incorrect interpretation of claim 5.

As Patent Owner explained in its preliminary response, claim 5 requires activation of account access in response to generation of the claimed “new password.” *See* Paper 8, pp. 30-31. But the Board disagreed:

We disagree with Patent Owner’s arguments. Claim 5 requires that the account be activated in response to the password. Ex. 1001, 12:41–43. It does not require that the account be activated in response to creation of the password. *Id.* On the record before us, Petitioner has adequately demonstrated that Veneklasé discloses activation of the account in response to the password. *See* Pet. 41–42.

Paper 9, p. 24. The Board’s interpretation of claim 5 is incorrect for the following reasons.

The plain language of claim 5 requires activation of account access in response to generation of the claimed “new password.” *See* Ex. 2003, ¶¶65-67. The relevant portions of claim 5 are reproduced below:

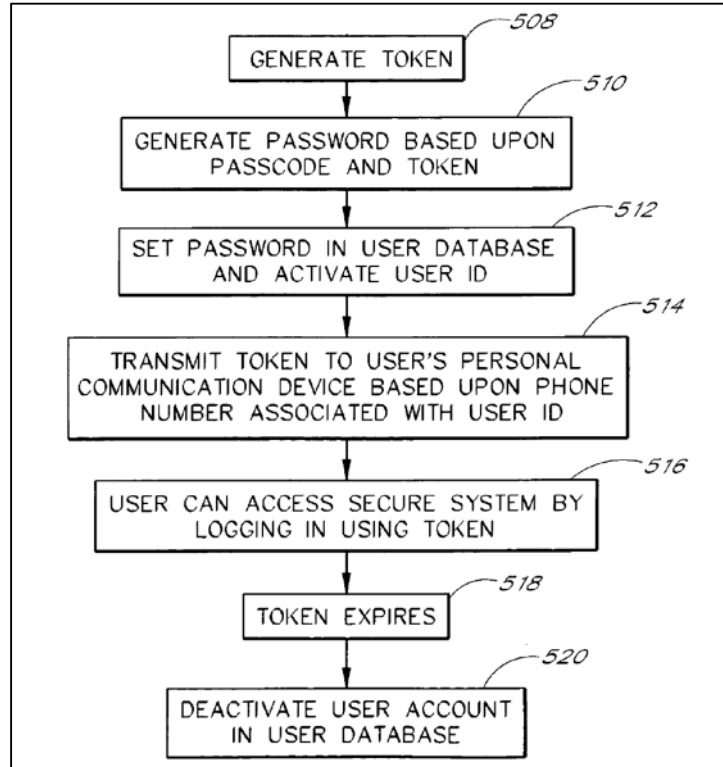
a control module executed on the computer processor configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a password associated with the user 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). 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.* So 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.*; Ex. 2003, ¶¶65-67.

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*; Ex. 2003, ¶¶65-67. Patent Owner’s interpretation of claim 5 is also consistent with the preliminary construction issued by the Eastern District of Texas on October 5:

C	“activates access to the account in response to the password” (Claim 5)	“activates access to the account in response to the creation of the password”
---	--	---

Ex. 2002. The Board is required to apply the same claim-construction standard as in Federal district court.

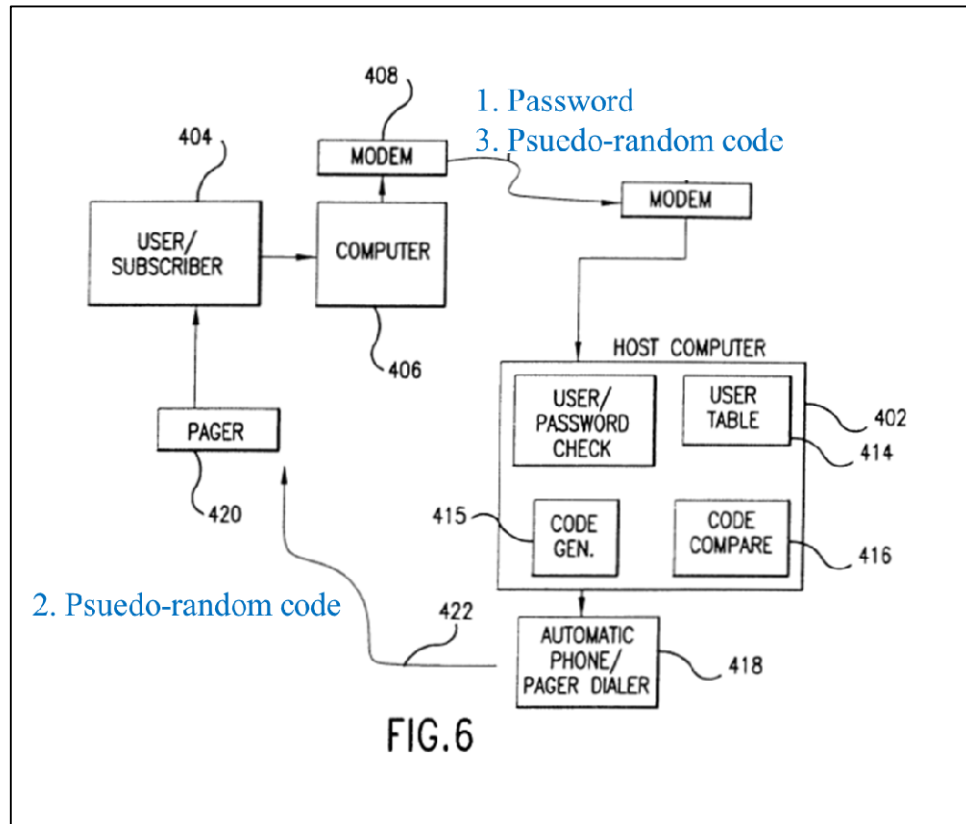
Accordingly, Patent Owner respectfully requests that the Board find that claim 5 requires activation of account access in response to generation of the claimed “new password,” and that the Board apply that finding to the grounds asserted by Petitioner.

V. RESPONSE TO ISSUES RAISED IN THE PETITION AND THE INSTITUTION DECISION

A. Ground 1 – The Combination of Veneklase and Jonsson Does Not Render Obvious Claim 5 of the ’658 Patent.

Petitioner contends that the combination of *Veneklase* and *Jonsson* renders obvious claim 5 of the ’658 Patent. Pet. at 2, 13-46. That combination does not render obvious claim 5 of the ’658 Patent for at least the following reasons.

Veneklase discloses a computer security system including a user’s “computer 406,” a user’s “pager 420,” and a “host computer 402.” Ex. 1005, 7:29-51, Fig. 6. Figure 6 of *Veneklase* is reproduced below:



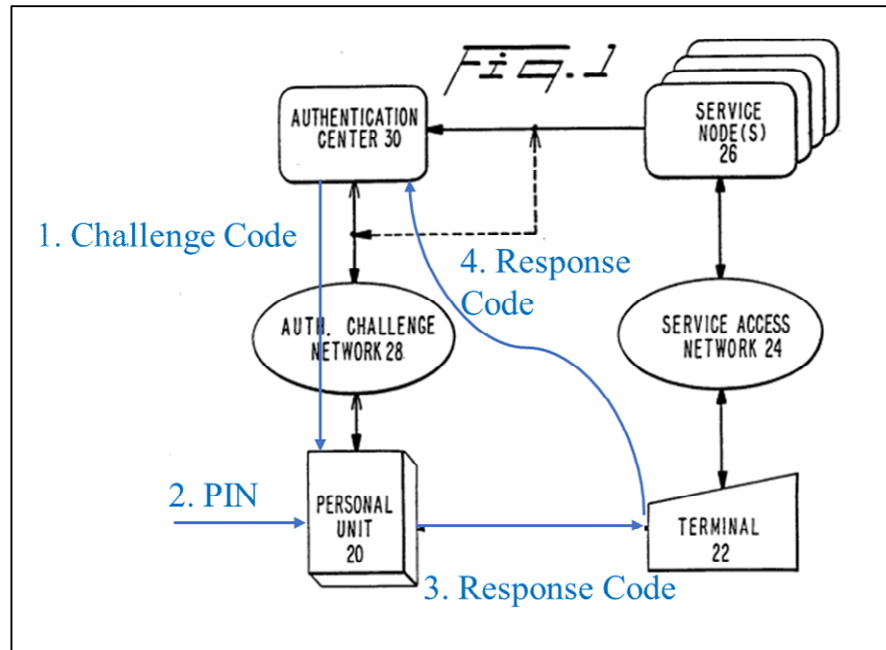
Ex. 1005, Fig. 6 (annotated and cropped). During an authentication process, the user transmits a “password” from “computer 406” to “host computer 402.” Ex. 1005, 7:58-8:27. “Host computer 402” then “cross references the received password [] against a pager phone number list” stored within “host computer 402.” *Id.* The “pager phone number list” stores the passwords of authorized users and the pager numbers for the authorized users. *See id.*, 6:10-26, Fig. 5. Assuming the user is an authorized user, the pager number for user’s “pager 420” would be associated with the user’s “password” in the “pager phone number list.” *See id.* A “pseudo-random code” is generated by “host computer 402” and transmitted to user’s “pager 420” using the pager number in the “pager phone number list” associated with the

“received password.” *See id.*, 8:1-26. Accordingly, *Veneklase*’s computer security system needs the user’s “password” to trigger generation of the “pseudo-random code” and to transmit the “pseudo-random code” to the user’s “pager 420.”

The user’s “pager 420” displays the received “pseudo-random code” to the user. *See id.*, 8:15-26. The user “enters the [pseudo-random] code he or she has received from the pager 420” into user “computer 406.” *Id.* The user-entered “pseudo-random code” is transmitted “back to computer 402, where it is compared” with the “pseudo-random code” sent to the user’s “pager 420.” *See id.* “If the comparison yields a match, the user 404 is allowed access to computer 402.” *Id.*, 8:25-27.

Accordingly, *Veneklase*’s system allows for authentication through user input of a password and a pseudo-random code at separate times in a two-step process. This 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.

Jonsson discloses a user authentication apparatus including a “service node 26,” an “authentication center 30,” a “personal unit 20,” and a user “terminal 22.” *See* Ex. 1006, 9:1-10:2, Fig. 1. Figure 1 of *Jonsson* is reproduced below:



Ex. 1006, Fig. 1 (annotated). In *Jonsson*'s authentication process, "authentication center 30" generates a "challenge code" and sends the "challenge code" to the "personal unit 20." Ex. 1006, 9:1-7. When the personal unit 20 receives the challenge code, "it prompts the user to input a PIN" and "generates a response code" using a stored algorithm that utilizes the PIN as an input. *Id.*, 9:9-25. But the "challenge code" is not displayed to the user. *See id.* Instead, the calculated "response code" is displayed to the user "for manual input to terminal 22." "Terminal 22" transmits the "response code" back to "authentication center 30" which may then compare the response code to [an] expected response." *Id.*, 9:26-10:1. If there is a match between the received "response code" and the "expected response," the "service node 26 permits the user to access the services offered." *Id.*

1. Independent Claim 5

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.

- i. [5.3] “a control module . . . configured to create a new password based at least upon a token and a passcode”

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 Petitioner’s proposed combination fails to support a conclusion of obviousness for multiple reasons. *See* Ex. 2003, ¶72.

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). See Ex. 2003, ¶73.

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; see Ex. 2003, ¶74.

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). *See* Ex. 2003, ¶75.

But modifying *Veneklase’s* system by abolishing the two-step authentication process, as proposed by Petitioner, would violate *Veneklase’s* principle of operation. *See* Ex. 2003, ¶76. *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. *See* Ex. 2003, ¶76. Accordingly, this two-step authentication process is a key feature of *Veneklase’s* principle of operation, and a POSITA would not seek to remove steps as Petitioner proposes. *See* Ex. 2003, ¶76. The Board found in the Institution Decision that “Patent Owner has not adequately demonstrated that the two-step authentication process is a key feature of *Veneklase’s* principle of operation such

that the proposed modification would render Veneklase's system inoperable." Paper 9, p. 17. But *Veneklase* unequivocally states the opposite. See Ex. 1005, 7:16-28; Ex. 2003, ¶76.

Accordingly, 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. See Ex. 2003, ¶76. See MPEP § 2143.01(VI) (citing *In re Ratti*, 270 F.2d 810, 813 (CCPA 1959)) ("If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious."); see also *Plas-Pak Indus. v. Sulzer Mixpac AG*, 600 F. App'x. 755, 758 (Fed. Cir. 2015) ("combinations that change the basic principles under which the [prior art] was designed to operate or that render the prior art inoperable for its intended purpose may fail to support a conclusion of obviousness.") (cleaned up).

Petitioner also argues, contrary to its previous argument, 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, *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; Ex. 2003, ¶77.

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. Petitioner provides

zero evidence that the security of its proposed combination is superior to the existing multi-layer/level security in *Veneklase*. See Ex. 2003, ¶78. Accordingly, there is no motivation to combine *Veneklase* and *Jonsson*.

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 SIM swapping would also not work in *Veneklase*’s existing system because the hackers would still need *Veneklase*’s password. See Ex. 2003, ¶79. Further, as discussed below regarding claim element [5.4], the combined system would be more prone to Denial of Service (DoS) attacks by hackers. See Ex. 2003, ¶79. Accordingly, a POSITA would not consider the combined system to be superior to *Veneklase* in terms of security, and thus there is no motivation to combine *Veneklase* and *Jonsson*. See Ex. 2003, ¶79.

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. See Ex. 2003, ¶80.

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, 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. *See also* Ex. 2003, ¶81.

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

- ii. [5.4] “a communication module configured to transmit the token to the personal communication device through the cell phone network”

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. Petitioner’s argument is contrary to its own modifications to *Veneklase* that were necessary to allegedly meet the requirements of claim element [5.3]. *See* Ex. 2003, ¶83.

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. *See also* Ex. 2003, ¶84.

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. See also* Ex. 2003, ¶85.

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). 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. *See* Ex. 2003, ¶86. Thus, there is no motivation for the proposed modification: “If references taken in combination would produce a seemingly inoperative device, we have held that such references teach away from the combination and thus cannot serve as predicates for a *prima facie* case of obviousness.” *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 1354 (Fed. Cir. 2001) (cleaned up). This is a fatal defect in the Petition. *See* Ex. 2003, ¶86.

The Board rejected this argument in the Institution Decision:

We disagree with Patent Owner’s characterization of the proposed modification as it pertains to limitation [5.4]. It is our understanding that in the proposed combination the user’s device would be identified in accordance with Jonsson’s teachings not Veneklase’s. *See* Pet. 30–32. In other words, the user’s device would be identified in response to the user’s request for authentication as described in Jonsson. *See e.g.*, Ex. 1006, 9:2–8; 10:13–27, Fig. 3). Accordingly, the ability to look up the user’s phone number is not a requirement of the combination and Patent Owner’s argument is inapposite.

Paper 9, p. 21. As a threshold matter, with respect to the proposed combination, the Petition never expressly stated that the user’s device would be identified according to *Jonsson*’s teachings. *See* Pet. 30-32. But even if that is the case, *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. 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.” *See* Ex. 2003, ¶88.

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 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 a “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. *See* Ex. 2003, ¶89. Thus, Petitioner’s rationale for combining *Veneklase* and *Jonsson* is not actually realized, and a POSITA would not be motivated to execute the proposed combination. *See* Ex. 2003, ¶89.

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 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). If *Jonsson's* "authentication request" is not a password, then the proposed combination is open to Denial of Service attacks (DoS). *See* Ex. 2003, ¶90. This is a flaw in *Jonsson's* architecture and a flaw in the proposed combination. *See* Ex. 2003, ¶90. In contrast, *Veneklase's* system with its two passwords does not suffer from this flaw. Accordingly, there is no motivation to combine *Veneklase* and *Jonsson* as proposed by Petitioner. *See* Ex. 2003, ¶90.

In view of the above, 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.

- iii. [5.5] "an authentication module configured to receive the password from the user through a secure computer network"

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). Patent Owner disagrees. See Ex. 2003, ¶92.

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.”). See Ex. 2003, ¶93.

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. See also Ex. 2003, ¶94.

Petitioner conveniently glosses over 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, 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 Petitioner provides zero evidence that an off-the-shelf pager, in 1996, was capable of executing specialized security algorithms. See Ex. 2003, ¶95. 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; Ex. 2003, ¶95. *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); Ex. 2003, ¶95. 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 Veneklase’s pager 420, are capable of executing Jonsson’s algorithm.

Paper 9, p. 22. But the Board’s citation to *Jonsson* removes the important context of the preceding sentence. *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, there is zero evidence in the record that *Veneklase’s* “pager 420” is capable of executing such an algorithm. To the contrary, the evidence indicates that *Veneklase’s* “pager 420” is not capable of executing such an algorithm. *See* Ex. 2003, ¶96.

In view of the above, 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.

- iv. [5.6] “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”

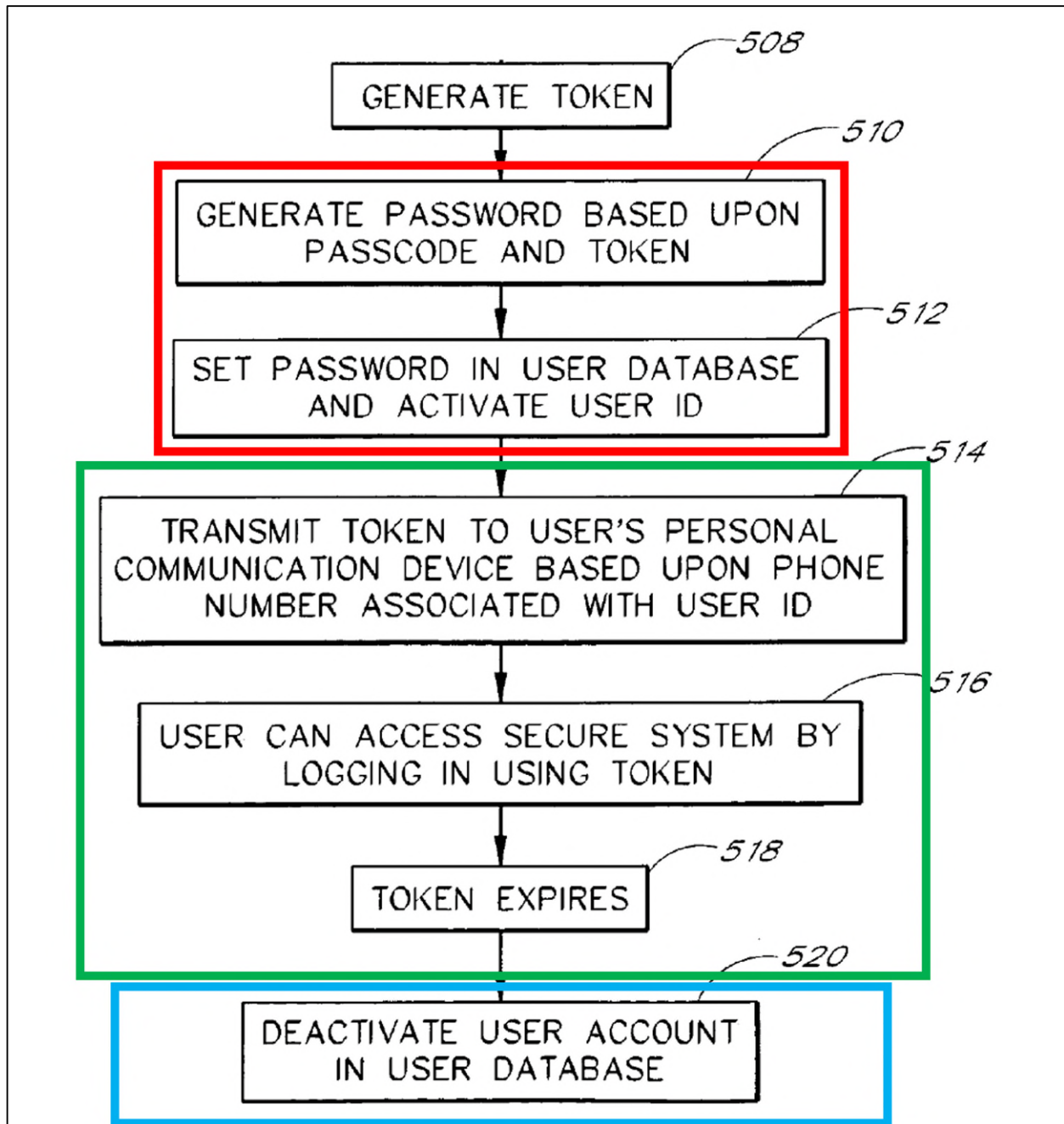
Claim element [5.6] recites “wherein the user has an account on the secure computer network, wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account, such that said account is not accessible through any password via the secure computer network.” Ex. 1001, 12:40-47 (emphasis added). As discussed above in Section IV, claim 5 requires activation of account access in response to generation of the claimed “new password.” See Ex. 2003, ¶98. The Preliminary Patent Owner Response identified two deficiencies in the Petition regarding this claim element. See Paper 8, pp. 31-32. The Institution Decision rejected Patent Owner’s arguments:

We disagree with Patent Owner’s argument. Claim 5 requires an authentication module that “deactivates the account within a predetermined amount of time after activating the account.” Ex. 1001, 12:43–54). It does not require that the predetermined amount of time correspond to the entire time period between activation and deactivation of the account. On the record before us, Petitioner has adequately demonstrated that Veneklasé discloses deactivation of the account within a predetermined amount of time. *See* Pet. 42–43.

Paper 9, p. 25 (emphasis added). But the Board’s rejection is based on incorrect interpretation of the plain language of claim 5, which is reproduced in pertinent part below:

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, 12:41-47 (emphasis added). The language of the claim is unequivocal: the “predetermined period of time” starts “after activating the account” and ends upon “deactivat[ion] [of] the account.” *See id.*; Ex. 2003, ¶98. 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. Petitioner’s arguments fail for the following reasons. *See* Ex. 2003, ¶98.

First, Petitioner argues that *Veneklase* 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 akin 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, 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. *See* Ex. 2003, ¶99.

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. 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; *See* Ex. 2003, ¶100.

Third, 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; Ex. 2003, ¶101.

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, 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. *See* Ex. 2003, ¶102.

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. See Ex. 2003, ¶103.

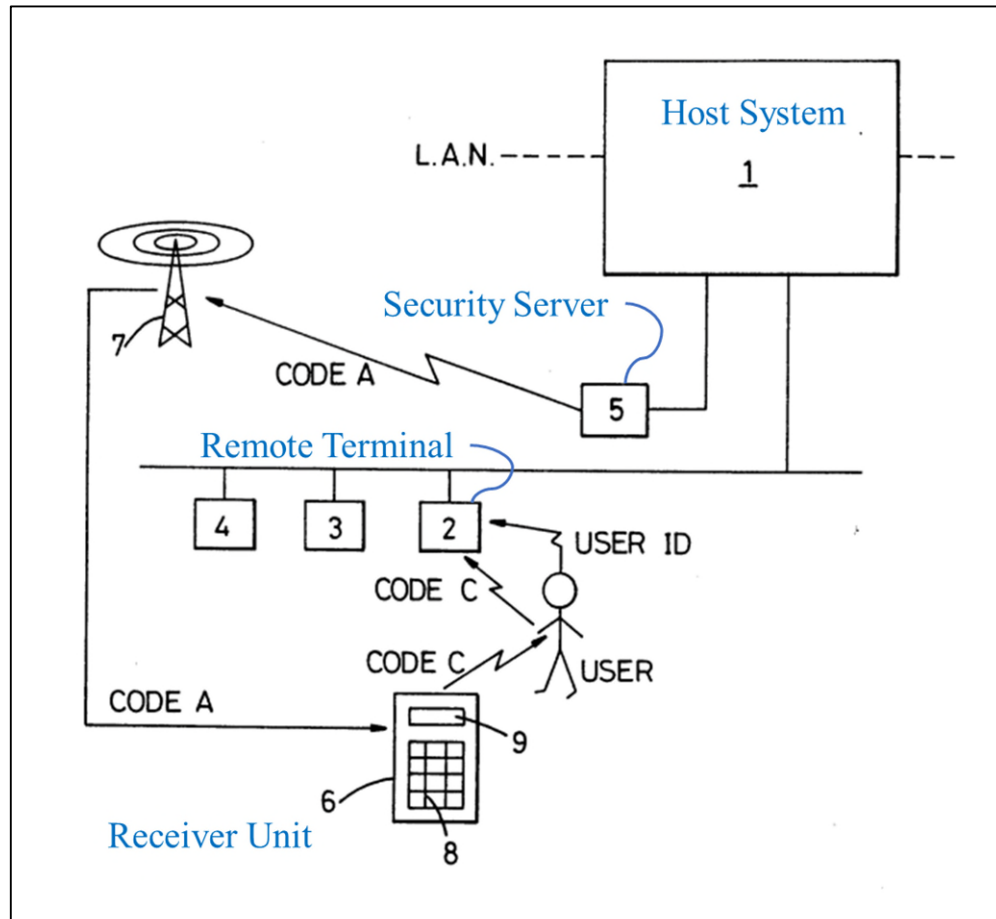
In view of the above, the combination of *Veneklase* and *Jonsson* fails to teach or suggest claim element [5.6], and thus fails to render claim 5 obvious.

B. Ground 2 – The Combination of Kew and Sormunen Does Not Render Obvious Claims 1 and 3-6 of the '658 Patent.²

Petitioner contends that the combination of *Kew* and *Sormunen* renders obvious claims 1 and 3-6 of the '658 Patent. Pet. at 2, 46-77. That combination does not render obvious claims 1 and 3-6 of the '658 Patent for at least the following reasons.

Kew discloses a computer security system including a “host system 1,” a “security server 5,” a “receiver unit 6,” and a “remote terminal 2.” Ex. 1007, 7:34-9:11, Fig. 1. Figure 1 of *Kew* is reproduced below:

² The Institution Decision does not contain any findings regarding the patentability challenged in Ground 2. See Paper 9, p. 25.



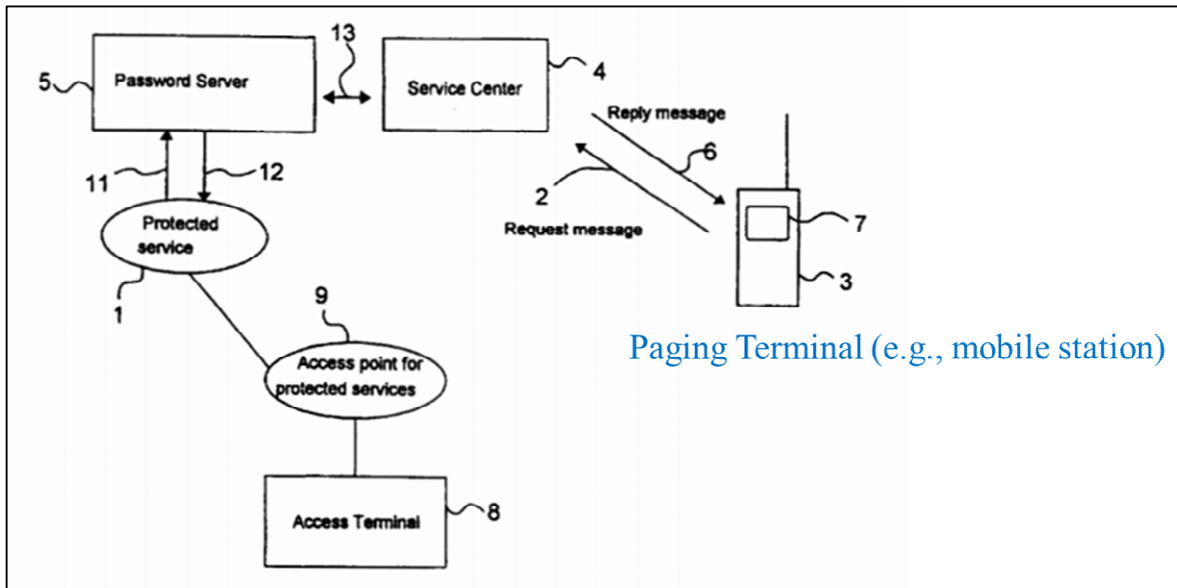
Ex. 1007, Fig. 1 (annotated). The user carries “receiver unit 6” which stores a one-way encryption algorithm and an “identity code.” The “identity code is a key for the one-way [encryption] algorithm.” Ex. 1007, 7:20-32. That code is stored in the EPROM of receiver unit 6. Ex. 1007, 7:28-29.

When “the user seeks access to the host system 1 via the terminal 2, he enters his user identification code . . . such as a PIN” for transmission to “security server 5.” *Id.*, 7:34-8:10. The “user identification code” (e.g., user PIN) is not the same as the “identity code” (i.e., encryption key) stored in “receiver unit 6.” *See* Ex. 1007, 11:5-11.

The “security server 5” includes a database storing the user identification codes (e.g., PINs) for all authorized users, the receiver unit for each authorized user, the identity of the one-way encryption algorithm executing on each receiver unit, and the identity code (i.e., encryption key) stored on each receiver unit. *See id.*, 7:34-8:10. The “security server 5” generates a random code (“Code A”), then generates a transformed code (“Code B”) by applying the same one-way encryption algorithm and identity code (i.e., encryption key) stored on “receiver unit 6” to “Code A.” *See id.* The “security server 5” also transmits “Code A” to the “receiver unit 6.” *See id.*, 8:11-23.

“Receiver unit 6” receives “Code A” and generates “Code C” by applying its stored “one-way [encryption] algorithm” with its “identity code” (i.e., encryption key) to “Code A.” “Code A” is not displayed on “receiver unit 6.” But “Code C” is displayed so that the user can input “Code C” into the “remote terminal” for transmission to the “security server 5.” *See id.*, 9:1-11. If “Code B and Code C are identical, access to host system 1 is permitted.” *Id.*

Sormunen discloses “a method for obtaining at least one item of user specific data, wherein the user specific data is obtained at least partly by using paging or a short message service.” Ex. 1008, Abstract. To obtain a password, “the user of the service sends a short message 2 from the paging terminal 3, such as a mobile station.” *Id.*, 5:35-38, Fig.2. Figure 2 of *Sormunen* is reproduced below.



Ex. 1008, Fig. 2 (annotated). The “short message 2 includes a password request.” *Id.*, 5:38-6:1. Then, the “paging service center 4 processes the incoming message and forms according to it a data transmission connection to a password server 5 and transmits the inquiry to it,” which “processes the message and forms a reply message containing one or more passwords.” *Id.*, 6:20-24. Finally, “the reply message 6 arrived to the paging terminal 3 can be shown to the user for example by the display means 7 of a mobile station used as a paging terminal” and “[t]he user may subsequently start using the service 1.” Ex. 1008, 8:4-7.

1. Independent Claim 5

The combination of *Kew* and *Sormunen* does not render obvious independent claim 5 because the combination does not teach or suggest the following elements of the claim. *See* Ex. 2003, ¶106.

- i. [5.3] “a control module . . . 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”

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.” Ex. 1001, 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. *See* Ex. 2003, ¶107.

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.

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." *See* Ex. 2003, ¶108.

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.” *See* Ex. 2003, ¶109.

Moreover, a POSITA would understand that the “identity code” would not be known to the user, as is required by the claim. *See* Ex. 2003, ¶111. 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. *See* Ex. 2003, ¶111. 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; *See* Ex. 2003, ¶111. The choice in *Kew* to store the “identity code” in EPROM, as opposed to RAM, 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.” *See* Ex. 2003, ¶111. 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. *See* Ex. 2003, ¶111. In such case the user’s knowledge of the “identity code” is not required. *See* Ex. 2003, ¶111. That is why a POSITA would understand that the “identity code” would not need to be known to the user, as is required by this claim element. *See* Ex. 2003, ¶111.

In an attempt at sleight of hand, the Petition misleadingly confounds 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. Here is what *Kew* actually says, without Petitioner’s fabrication:

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). 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. . . .”); Ex. 2003, ¶112; see also Ex. 1007, 11:8-11. Thus, Petitioner’s mischaracterization of the “identity code” is not correct.

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; *See* Ex. 2003, ¶113. 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; Ex. 2003, ¶113. 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; Ex. 2003, ¶113.

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; Ex. 2003, ¶114.

In view of the above, *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, the combination of *Kew* and *Sormunen* does not teach or suggest this claim element.

- ii. [5.6] “wherein the authentication module . . . deactivates the account within a predetermined amount of time after activating the account”

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). 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. . . .” Ex. 1001, 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):

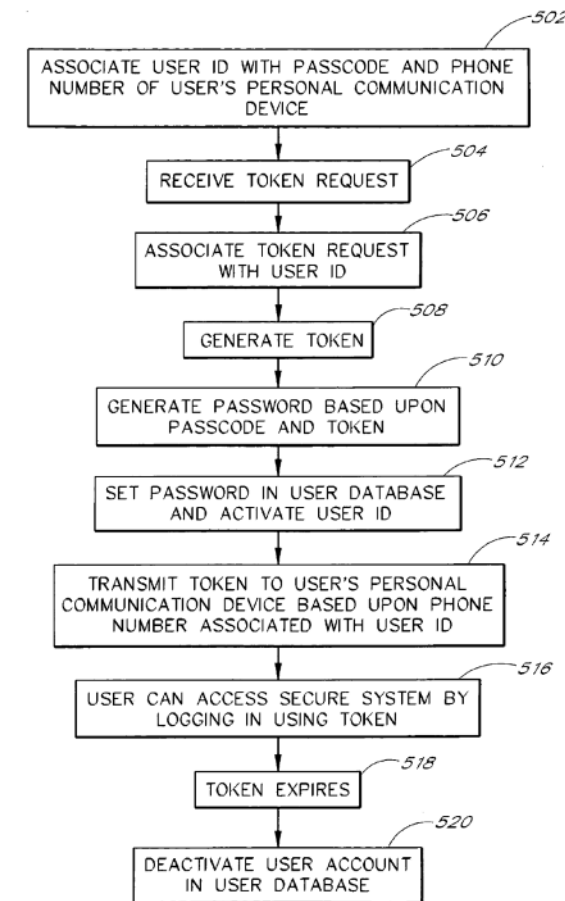


FIG. 5

Ex. 1001, 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.*; Ex. 2003, ¶116.

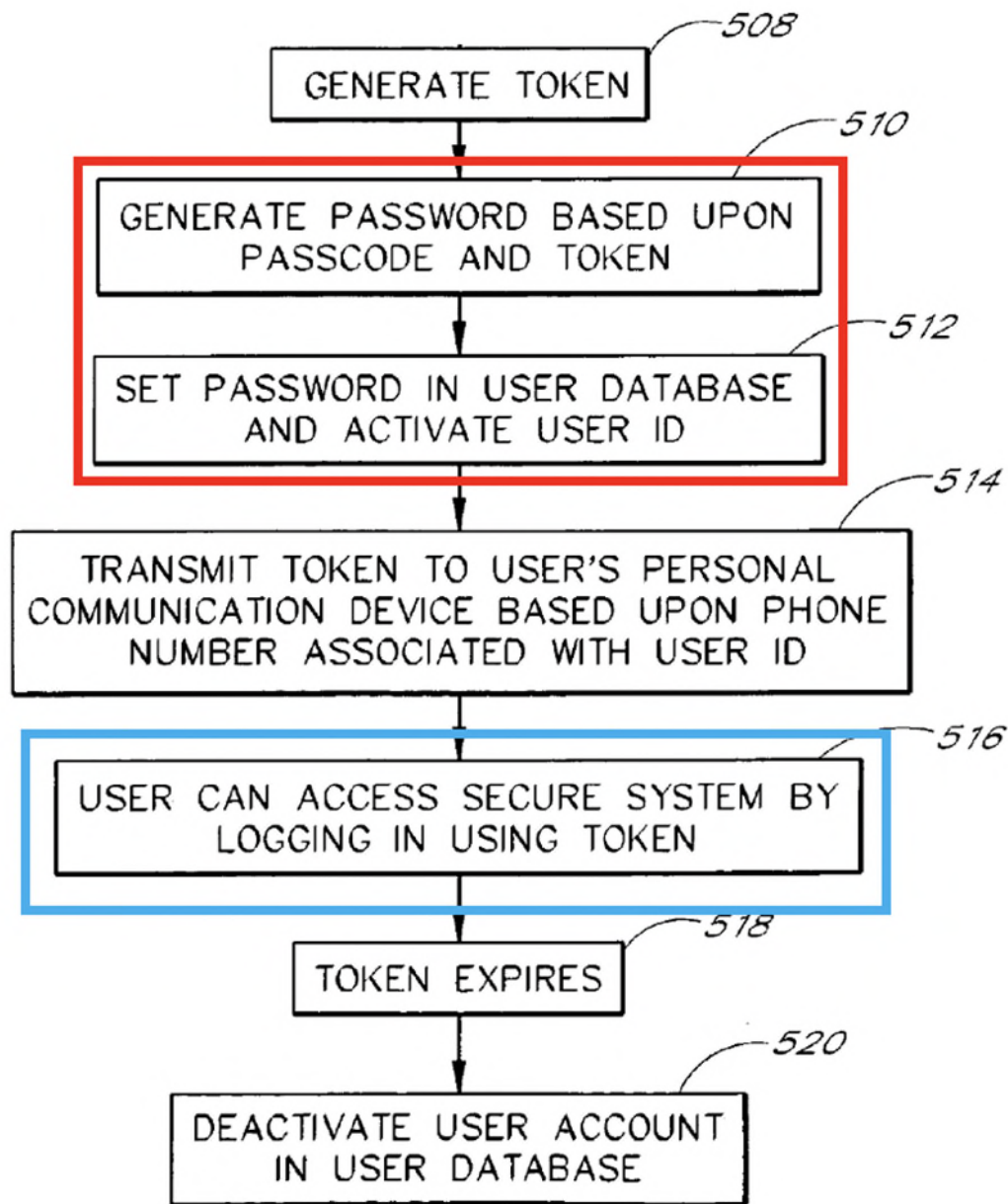
The Petition fails to show that *Kew* discloses activating account access in response to generation of the new “password,” which is “based at least upon a token and a passcode.” *See* Pet, pp. 67-72. The Petition alleges that the security server in *Kew* comparing the stored password with the password 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; *see* Ex. 2003, ¶117. 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. *See* Ex. 2003, ¶117. But 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:



Ex. 1001, 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* Ex. 1001, 9:28-43, Fig. 5. And that process occurs before the “token” is transmitted to the user in step 514. *See id.*; Ex. 2003, ¶117.

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, 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* 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, 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; Ex. 2003, ¶118.

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). 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 *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 See* Ex. 1007, 8:11-9:11, 12:6-13:6. The disclosures cited 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; Ex. 2003, ¶119. 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; Ex. 2003, ¶119. 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; Ex. 2003, ¶119. 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. *See* Ex. 2003, ¶119.

In view of the above, *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, the combination of *Kew* and *Sormunen* does not render independent claim 5 obvious.

2. Dependent Claim 6

Dependent claim 6 depends from and adds limitations to independent claim 5. 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. *See* Ex. 2003, ¶121.

3. Independent Claim 1

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. *See* Ex. 2003, ¶122.

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, 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, the combination does not render independent claim 1 obvious. *See* Ex. 2003, ¶123

- i. [1.2] “receiving a request from the user for a token via the personal communication device, over the second network”

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, 73, 74. *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. Petitioner's proposed combination of *Kew* and *Sormunen* fails to support a conclusion of obviousness for multiple reasons. *See* Ex. 2003, ¶124.

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, this sequence of events is fundamental to *Kew*'s authentication process and thus is a key feature of *Kew*'s principle of operation. *See* Ex. 2003, ¶125.

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, the proposed modification has no reasonable expectation of success, and does not render independent claim 1 obvious. *See Intelligent Bio-Systems, Inc. v. Illumina Cambridge, Ltd.*, 821 F.3d 1359, 1367 (Fed. Cir. 2016) ("One must have a motivation to combine accompanied by a reasonable expectation of achieving what is claimed" and "the Board conflated two different legal concepts—reasonable expectation of success and motivation to combine"). *See* Ex. 2003, ¶126.

Further, Petitioner's proposed modification changes the fundamental sequence of events in *Kew*'s authentication process. *See* Ex. 2003, ¶127. 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. *See* Ex. 2003, ¶127. *See also* MPEP

§ 2143.01(VI) (citing *In re Ratti*, 270 F.2d 810, 813 (CCPA 1959)) (“If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious.”); *see also Plas-Pak Indus. v. Sulzer Mixpac AG*, 600 F. App’x. 755, 758 (Fed. Cir. 2015) (“combinations that change the basic principles under which the [prior art] was designed to operate or that render the prior art inoperable for its intended purpose may fail to support a conclusion of obviousness.”) (cleaned up). *See* Ex. 2003, ¶127.

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”). *See* Ex. 2003, ¶128.

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. *See* Ex. 2003, ¶129.

Kew discloses the "user identification code" is "preferably a more secure code such as a PIN." Ex. 1007, 8:1-2. Increasing the number of times the "user identification code" is transmitted only increased the likelihood of it being intercepted. Accordingly, 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. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) ("Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness") (cleaned up) (emphasis added). *See* Ex. 2003, ¶130.

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

4. Dependent Claims 3 and 4

Dependent claims 3 and 4 depend from and add limitations to independent claim 1. 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. *See* Ex. 2003, ¶132.

VI. THE BOARD DOES NOT HAVE JURISDICTION OVER EXPIRED PATENTS.

In *Oil States*, the Supreme Court explained that the “decision to *grant* a patent is a matter involving public rights—specifically, the grant of a public franchise.” *Oil States Energy Servs., LLC v. Greene’s Energy Grp., LLC*, 138 S. Ct. 1365, 1373 (2018). “Specifically, patents are public franchises that the Government grants to the inventors of new and useful improvements.” *Id.* (internal quotation marks omitted). The Court explained that “Congress [has] significant latitude to assign [the] adjudication of public rights to entities other than Article III courts.” *Id.* at 1368. In exercising its “significant latitude,” Congress grants public franchises “subject to the qualification that the PTO has the authority to reexamine—and perhaps cancel—a patent claim in an inter partes review.” *Id.* at 1368, 1374 (internal quotation marks omitted). Accordingly, so long as the public franchise exists, the Patent Office may have jurisdiction to amend and cancel the claims of the patent (e.g., via *inter partes* review).

When a patent expires, however, the public franchise ceases to exist and the franchisee (e.g., the patent owner) no longer has the right to exclude others. At most, the franchisee may be entitled to collect damages from the public franchise that formerly existed through an infringement action in district court. But because the public franchise no longer exists, the Patent Office has nothing in its authority to

cancel or amend. Expiration removes the patent from the Patent Office's jurisdiction and returns it to the sole jurisdiction of the Article III courts, which have exclusive authority to govern claims for damages. If this were not so, the Patent Office would purport to have authority to retroactively modify a public franchise that no longer exists, in a setting where the expired public franchise does not enjoy any presumption of validity and in which amendment of claims is no longer permitted.

The '658 Patent issued in January 2006 and expired in March 2020, long before the Petition was filed on January 6, 2023. With the expiration of the '658 Patent in March 2020, the Board ceased to have jurisdiction over the '658 Patent, and this *inter partes* review proceeding should be terminated as a result.

VII. CONCLUSION

For the foregoing reasons, Petitioner has not established that the cited references render any of the challenged claims unpatentable.

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(d), I hereby certify that the foregoing Patent Owner Response contains 11,878 words as measured by the word processing software used to prepare the document, excluding the cover page, signature block, and portions exempted under 37 C.F.R. § 42.24(a) or (b).

DATED: October 10, 2023

Respectfully submitted,

By: /John Wittenzellner/
John Wittenzellner
Registration No. 61,662
Counsel for Patent Owner

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6, the undersigned certifies that on October 10, 2023, the foregoing document was served on counsel of record for Petitioner by filing this document through the End-to-End System, as well as via electronic mail to counsel of record for Petitioner at the following addresses: Timothy J. Murphy (tj@unifiedpatents.com), Jordan M. Rossen (jordan@unifiedpatents.com), and Ashraf Fawzy (afawzy@unifiedpatents.com).

Respectfully submitted,

By: /John Wittenzellner/
John Wittenzellner
Registration No. 61,662
Counsel for Patent Owner