

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

AMAZON.COM, INC.,
Petitioner,

v.

DYNAPASS IP HOLDINGS, LLC,
Patent Owner.

***Inter Partes* Review No. IPR2024-00283**
Patent No. 6,993,658

PATENT OWNER'S PRELIMINARY RESPONSE
UNDER 37 C.F.R. § 42.107

Filed on behalf of Patent Owner by:

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

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

Michael J. Fagan, Jr.
2633 McKinney Ave., Suite 130
Dallas, TX 75204

WILLIAMS SIMONS & LANDIS PLLC

TABLE OF CONTENTS

I.	INTRODUCTION	2
II.	STATEMENT OF THE PRECISE RELIEF REQUESTED	3
III.	THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY THE PETITION.	4
A.	The Board Should Deny the Petition Under 35 U.S.C. § 325(d).	4
1.	The First Part of the Framework is Satisfied.	4
2.	The Second Part of the Framework is Also Satisfied.	7
B.	The Board Should Deny the Petition Under 35 U.S.C. § 314(a).	7
1.	<i>General Plastic</i> Factor One	8
2.	<i>General Plastic</i> Factor Two	10
3.	<i>General Plastic</i> Factor Three	11
4.	<i>General Plastic</i> Factors Four and Five	12
5.	<i>General Plastic</i> Factor Six and Seven	13
IV.	THE PETITION SHOULD BE DENIED BECAUSE IT DOES NOT ESTABLISH A REASONABLE LIKELIHOOD OF SUCCESS ON ANY CHALLENGED CLAIM	14
A.	The '658 Patent	14
B.	Level of Ordinary Skill in the Art	22
C.	Claim Construction	22

D.	Cited Art	23
E.	Ground 1 – The Combination of <i>Veneklase, Jonsson</i> , and <i>Sormunen</i> Does Not Render Obvious Dependent Claim 7.....	31
1.	Independent Claim 5	31
i.	5[c] “a control module . . . configured to create a new password based at least upon a token and a passcode” ..	31
ii.	5[d] “a communication module configured to transmit the token to the personal communication device through the cell phone network”	37
iii.	5[e] “an authentication module configured to receive the password from the user through a secure computer network”	41
iv.	5[f] “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”	43
2.	Dependent Claim 6.....	49
3.	Dependent Claim 7.....	51
F.	Ground 2 – The Combination of <i>Veneklase, Jonsson, Sormunen</i> , and <i>Kaufman</i> Does Not Render Obvious Dependent Claim 2.....	54

1.	Independent Claim 1	54
2.	Dependent Claim 2.....	55
G.	Ground 3 – The Combination of <i>Kew</i> and <i>Sormunen</i> Does Not Render Obvious Dependent Claim 7.....	58
1.	Independent Claim 5	58
i.	5[c] “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”	58
ii.	5[f] “wherein the authentication module . . . deactivates the account within a predetermined amount of time after activating the account”	63
2.	Dependent Claim 7.....	65
H.	Ground 4 – The Combination of <i>Kew</i> , <i>Sormunen</i> , and <i>Kaufman</i> Does Not Render Obvious Dependent Claim 2.	69
1.	Independent Claim 1	69
2.	Dependent Claim 2.....	70

TABLE OF AUTHORITIES

Cases

<i>Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH</i> , IPR2019-01469, Paper 6 (P.T.A.B. Feb. 13, 2020) (precedential).....	4, 7
<i>Code200, UAB v. Bright Data Ltd.</i> , IPR2022-00861, Paper 18 (P.T.A.B. Aug. 23, 2022) (precedential).....	12
<i>Cuozzo Speed Techs., LLC v. Lee</i> , 136 S. Ct. 2131 (2016)	7
<i>Ericsson Inc. v. Uniloc 2017, LLC</i> , IPR2019-01550, Paper 8 (Mar. 17, 2020).....	8
<i>General Plastic Indus. Co. v. Canon Kabushiki Kaisha</i> , IPR2016-01357, Paper 19 (P.T.A.B. Sept. 6, 2017) (precedential).....	8
<i>In re Ratti</i> , 270 F.2d 810 (CCPA 1959).....	33, 66
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007)	67
<i>McGinley v. Franklin Sports, Inc.</i> , 262 F.3d 1339 (Fed. Cir. 2001).....	39
<i>Meiresonne v. Google, Inc.</i> , 849 F.3d 1379 (Fed. Cir. 2017).....	56
<i>Valve Corp. v. Electronic Scripting Products, Inc.</i> , IPR2019-00064, Paper 10 (P.T.A.B. May 1, 2019) (precedential).....	13
<i>Valve Corporation v. Electronic Scripting Products, Inc.</i> , IPR2019-00062, Paper 11 (P.T.A.B. April 2, 2019) (precedential)	8, 14

Statutes

35 U.S.C. § 112.....	31, 54, 58, 69
35 U.S.C. § 314.....	2, 7

35 U.S.C. § 316.....	2
----------------------	---

Other Authorities

MPEP § 2143.01	33, 66
----------------------	--------

Regulations

37 C.F.R. § 42.100	2, 22
--------------------------	-------

EXHIBIT LIST

Exhibit	Description
2001	Email authorizing Patent Owner to file a Motion for Additional Discovery (Mar. 21, 2024).
2002	Dynapass IP Holdings LLC’s Discovery Requests to Petitioner.
2003	Email correspondence between Patent Owner and Petitioner regarding Patent Owner’s request that Petitioner identify whether it has ever been a direct or indirect member of Unified Patents.
2004	https://www.unifiedpatents.com/success .
2005	Google Patents webpage for U.S. Patent No. 6,993,658, https://patents.google.com/patent/US6993658B1/
2006	U.S. Patent No. 6,173,400 (“ <i>Perlman</i> ”)
2007	U.S. Patent 7,058,974 (“ <i>Maher</i> ”)
2008	Microsoft Computer Dictionary (5th ed. 2002)

I. INTRODUCTION

Dynapass IP Holdings, LLC (“Patent Owner”) respectfully submits this Preliminary Response (the “Response”) to the Petition for *Inter Partes* Review of U.S. Patent No. 6,993,658 (IPR2024-00283, the “Petition” or “Pet.”) filed by Amazon.com, Inc. (“Petitioner”).

This Petition puts forth the same arguments and art as IPR2023-00425 filed by Unified Patents, but challenges different claims: IPR2023-00425 challenged claims 1 and 3-6, whereas this Petition challenges dependent claims 2 and 7 (the “Challenged Claims”) on the same art, as well as an additional prior-art reference for dependent claim 2. Petitioner concedes that by “adopting substantially the same unpatentability grounds and arguments, the Board’s analysis of independent claims 1 and 5 in conjunction with [*Unified Patents, LLC v. Dynapass IP Holdings LLC*, IPR2023-00425, (P.T.A.B. Jan. 6, 2023) (“Unified IPR”)] will apply here as well, thus eliminating the need for the Board to re-analyze those independent claims.” Pet., p. 1 (emphasis added). Patent Owner notes under 35 U.S.C. § 316(a)(11), a Final Written Decision for the Unified IPR is expected on or before July 18, 2024, whereas under 35 U.S.C. § 314(b) an institution decision in this proceeding is not due until July 22, 2024. Accordingly, Patent Owner respectfully submits that the Board’s Final Written Decision in IPR2023-00425 with respect to independent

claims 1 and 5 may warrant denial of institution of this Petition if those claims are found not unpatentable.

Institution should be denied because Petitioner has not established that the cited references render the Challenged Claims unpatentable. Additionally, or alternatively, the Board should deny the Petition under 35 U.S.C. §§ 314(a) and/or 325(d).

II. STATEMENT OF THE PRECISE RELIEF REQUESTED

Petitioner asserts that the Challenged Claims are unpatentable under the following grounds:

Ground	Prior Art	Statutory Basis	Claim
1	<i>Veneklase</i> in view of <i>Jonsson</i> and <i>Sormunen</i>	§ 103	7
2	<i>Veneklase</i> in view of <i>Jonsson</i> , <i>Sormunen</i> , and <i>Kaufman</i>	§ 103	2
3	<i>Kew</i> in view of <i>Sormunen</i>	§ 103	7
4	<i>Kew</i> in view of <i>Sormunen</i> and <i>Kaufman</i>	§ 103	2

Pet., p. 6. Patent Owner requests that the Board deny institution of the Petition with respect to all Challenged Claims and all asserted grounds. A full statement of the reasons for the relief requested is set forth in Sections III-IV of this Response.

III. THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY THE PETITION.

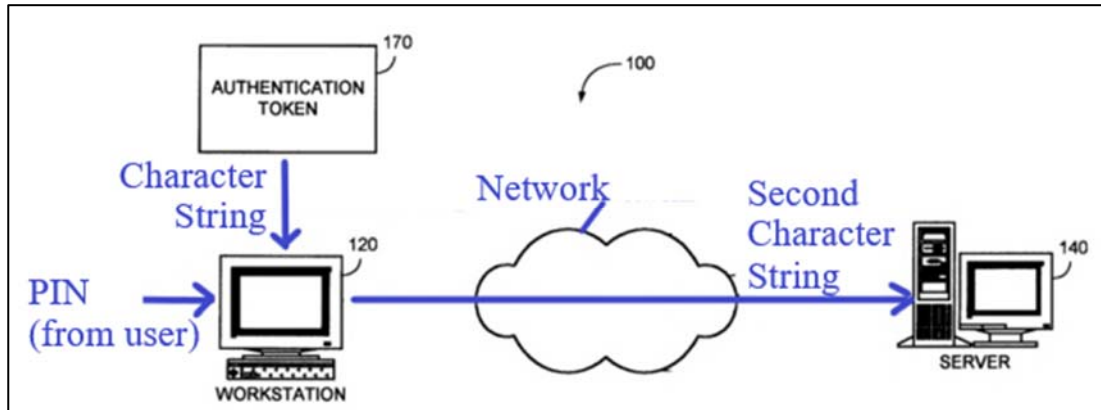
A. The Board Should Deny the Petition Under 35 U.S.C. § 325(d).

The USPTO evaluates Section 325(d) using a “two-part framework.” *See Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 at 8-9 (P.T.A.B. Feb. 13, 2020) (precedential).

1. The First Part of the Framework is Satisfied.

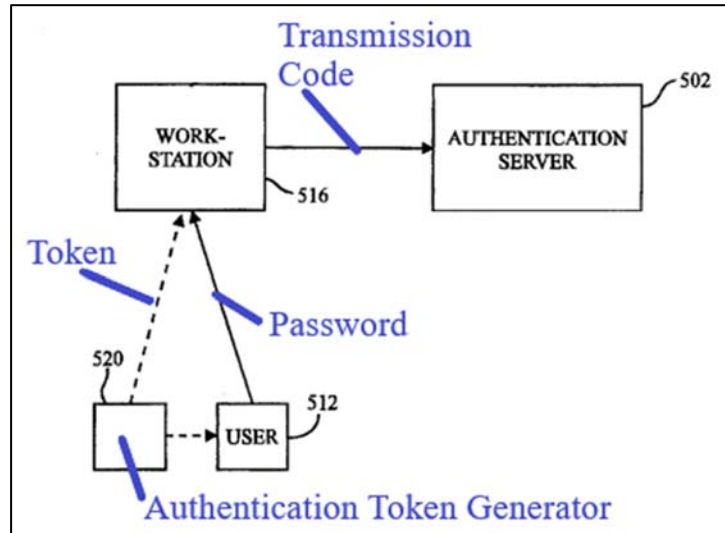
Veneklase, Jonsson, Sormunen, and *Kew* were previously presented to the USPTO in the Unified IPR. *Sormunen* was also presented to the Office in two additional IPRs challenging the ’658 Patent, where the Board considered the merits of *Sormunen* and ultimately denied institution. *See Bank of America, N.A. v. Dynapass IP Holdings LLC*, IPR2023-00367 (P.T.A.B. July 18, 2023) (“BOA IPR”); *Experian Information Solutions, Inc. v. Dynapass IP Holdings LLC*, IPR2023-01406 (P.T.A.B. March 28, 2024) (“Experian IPR”).

Further, *Kaufman* is substantially the same as U.S. Patent No. 6,173,400 (“*Perlman*”), which was both relied upon in the Experian IPR and considered by the Examiner during prosecution of the ’658 Patent. *See Experian IPR*, Paper 2 at 15, 49 (P.T.A.B. Sept. 28, 2023). *Perlman* discloses a “system 100” including an “authentication token 170,” a “workstation 120” and a “server 140.” EX2006, 4:65-5:8, Fig. 1. Figure 1 of *Perlman* is reproduced below:



EX2006, Fig. 1 (excerpted and annotation). *Perlman* discloses generating a “character string” using time-synchronized “authentication token 170.” *See id.*, 4:38-55, 8:55-9:19, Fig. 1. The “character string” is communicated to “workstation 120” along with a “PIN” provided by the user. *See id.* The “workstation 120” generates a “second character string” by executing a hash of the “character string” concatenated with the “PIN.” *See id.* The “workstation 120” transmits the “second character string” to “server 140” to authenticate the user. *See id.*

In comparison, *Kaufman* discloses a security system including an “authentication token generator 520,” a “workstation 516,” and an “authentication server 502.” EX1008, Abstract, Fig. 5. Figure 5 of *Kaufman* is reproduced below:



Id., Fig. 5 (excerpted and annotated). The “workstation 516” generates a “transmission code” based on a “password” entered by the user and a “token” generated by “authentication token generator 520.” *See id.*, 9:15-10:7. The “transmission code” is calculated by hashing a concatenation of the “password” and the “token.” *See id.* The “transmission code” is transmitted to the “authentication sever 502” and the user is granted access to the system if the “authentication server 502” can validate the received “transmission code.” *See id.*, 10:46-11:25.

Both *Perlman* and *Kaufman* employ an authentication token generator for authenticating a user. *Compare* EX2006, 4:38-55, 8:55-9:35, Fig. 1 *with* EX1008, 9:15-10:7, Fig. 5. In both *Perlman* and *Kaufman*, a workstation executes a hash of a user’s PIN/password concatenated with a string/token from the authentication token generator. *Compare* EX2006, 4:38-55, 8:55-9:35, Fig. 1 *with* EX1008, 9:15-10:7. In both *Perlman* and *Kaufman*, the hashed value is transmitted to an

authentication server to validate the user. *Compare* EX2006, 4:38-55, 8:55-9:35, Fig. 1 *with* EX1008, 10:46-11:25. Accordingly, *Perlman* and *Kaufman* are substantially the same. In fact, both *Perlman* and *Kaufman* were cited to disclose concatenating the user's passcode with a token, as claim 2 requires. *Compare* Pet., pp. 50-51 *with* Experian IPR, Paper 2 at 41-42 (P.T.A.B. Sept. 28, 2023).

The first part of the § 325(d) framework is therefore satisfied for every reference cited in the Petition.

2. The Second Part of the Framework is Also Satisfied.

The second part of the framework is satisfied because Petitioner fails to allege, much less demonstrate, that “the Office erred in a manner material to the patentability of challenged claims.” *Advanced Bionics*, Paper 6 at 8-9. Petitioner has not alleged that the Office erred in its evaluation of *Veneklase*, *Jonsson*, *Sormunen*, *Kew* or *Perlman* (and thus *Kaufman*). To the contrary, Petitioner concedes there is no “need for the Board to re-analyze those independent claims” of the '658 Patent. Pet., p. 1. Accordingly, the second part of the framework is also satisfied, and institution should be denied under 35 U.S.C. § 325(d).

B. The Board Should Deny the Petition Under 35 U.S.C. § 314(a).

The Board has discretion as to whether to institute *inter partes* review. *See* 35 U.S.C. § 314(a); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2140 (2016).

In *General Plastic*, the Board recognized “the potential for abuse of the review process by repeated attacks on patents.” *General Plastic Indus. Co. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 at 17 (P.T.A.B. Sept. 6, 2017) (precedential). To mitigate such abuse, the Board identified seven factors that it considers in determining whether to institute decision of a subsequent petition. *Id.*, Paper 19 at 16. In the present case, the *General Plastic* factors overwhelmingly favor denying institution.

1. *General Plastic* Factor One

In *Valve Corporation*, the Board clarified that “application of the *General Plastic* factors is not limited solely to instances when multiple petitions are filed by the same petitioner. Rather, when different petitioners challenge the same patent, [the Board considers] any relationship between those petitioners when weighing the *General Plastic* factors.” *Valve Corporation v. Electronic Scripting Products, Inc.*, IPR2019-00062, Paper 11 at 9 (P.T.A.B. April 2, 2019) (precedential) (emphasis added). In *Ericsson Inc. v. Uniloc*, the Board weighed the first *General Plastic* factor against institution because “[t]he instant Petitioner’s decision to use the prior petitions as a roadmap for its own petition ties the interests of all the petitioners together.” *Ericsson Inc. v. Uniloc 2017, LLC*, IPR2019-01550, Paper 8 at 12 (Mar. 17, 2020).

The first *General Plastic* factor weights heavily in favor of denying institution because the instant Petition was filed with the benefit of the BOA IPR Institution Decision, the Unified IPR Institution Decision, the Unified IPR Patent Owner Response, and the Experian IPR Petition. In other words, the instant Petition is the fourth attack on the '658 Patent. Like the instant Petition, the BOA IPR and the Experian IPR challenged at least claims 2 and 7 of the '658 Patent. *Compare* Pet., p. 6 with IPR2023-00367, Paper 1 at 1 (P.T.A.B. Jan. 3, 2023) and IPR2023-01406, Paper 2 at 15 (P.T.A.B. Sept. 28, 2023). The Unified IPR challenged at least claims 1, 5, and 6 of the '658 Patent. *See* IPR2023-00425, Paper 1 at 2 (P.T.A.B. Jan. 6, 2023). And under 35 U.S.C. § 112, ¶4, challenged claim 2 of the instant Petition necessarily incorporates all the limitations of claim 1, while challenged claim 7 necessarily incorporates all the limitations of claims 5 and 6.

There is also a significant relationship between Petitioner and the petitioners of the BOA IPR, the Experian IPR, and the Unified IPR¹ because all were sued by Patent Owner for infringement of the '658 Patent in the same district court. *See* Pet., pp. 2-4. Petitioner even admits those lawsuits are related cases. *Id.* Accordingly,

¹JPMorgan Chase Bank was joined as a petitioner to the Unified IPR via Motion for Joinder. *See* IPR2023-00425, Paper 17 (P.T.A.B. Jan. 19, 2024).

the overlap in the challenged claims and the significant relationship between all the petitioners favor denying institution.

2. General Plastic Factor Two

Here, Petitioner knew or should have known of the prior art references in the Petition—*Veneklase*, *Jonsson*, *Kew*, *Sormunen*, and *Kaufman*—when the Unified IPR Petition filed. That is because *Veneklase*, *Jonsson*, *Kew*, and *Sormunen* were cited in the Unified IPR Petition (IPR2023-00425, Paper 1 at 2 (P.T.A.B. Jan. 6, 2023)), while *Kaufman*, *Kew*, and *Sormunen* were already cited in the slightly older BOA IPR Petition (IPR2023-00367, Paper 1 at 11, 12, 80 (P.T.A.B. Jan. 3, 2023)).

The BOA IPR Institution Decision and the Unified IPR Institution Decision issued approximately five months after Petitioner was served with the complaint. Petitioner then waited an additional five months to file the instant Petition. As discussed above, Petitioner and the petitioners in the BOA IPR and Unified IPR were sued for infringement of the '658 Patent in the same district court. Petitioner even admits it was aware of those lawsuits. Pet., pp. 2-4. Accordingly, Petitioner and the petitioners of the BOA IPR and the Unified IPR are similarly situated. Petitioner knew or should have known of the prior art references in the Petition around the time the BOA IPR and Unified IPR filed (i.e., early January 2023). This factor favors denying institution.

3. *General Plastic Factor Three*

Regarding the Unified IPR, Patent Owner's preliminary response was filed on April 25, 2023, the Board instituted on July 18, 2023, and Patent Owner's response was filed on Oct. 10, 2023. Regarding the BOA IPR, Patent Owner's preliminary response was filed on April 27, 2023, and the Board denied institution on July 18, 2023. The Petition was filed five months later on December 28, 2023. Accordingly, Petitioner had access to Patent Owner's preliminary responses, Patent Owner's response, and the Board's decisions well before filing the Petition and thus would have been aware of Patent Owner's and the Board's arguments and positions. This factor favors denying institution.

Petitioner argues that it "is not using this Petition to address any deficiencies that have been alleged concerning the grounds raised in those [earlier IPR] proceedings." Pet., p. 8. But that is simply not true. In the BOA IPR, the Board found the combination of *Sormunen* and *Guthrie* insufficient to meet the limitations of challenged claims 2 and 7. See IPR2023-00367, Paper at 13 at 18. In response to that institution denial, Petitioner kept *Sormunen* but replaced *Guthrie* with other references (e.g., *Kew*, *Veneklase*, *Jonsson*, or *Kaufman*) to once again try to meet the limitations of challenged claims 2 and 7. *Kew*, *Veneklase*, and *Jonsson* were undoubtedly selected due to the Board instituting the Unified IPR, which relied on

those references. As explained by Petitioner, “road-mapping concerns are minimized when a petitioner files a later petition that raises unpatentability challenges substantially overlapping with those in the previously-filed petition and the later petition is not refined based on lessons learned from later developments.” Pet., p. 9 (quoting *Code200, UAB v. Bright Data Ltd.*, IPR2022-00861, Paper 18 at 5 (P.T.A.B. Aug. 23, 2022) (precedential)) (cleaned up). But Petitioner concedes that the instant Petition does not raise unpatentability challenges that substantially overlap those in the BOA IPR. See Pet., p. 9 n.3 (“Petitioner’s grounds are different from those raised in the [BOA IPR]”). Further, the instant Petition is refined based on lessons “learned from later developments” (i.e., successful institution of the Unified IPR citing *Veneklase, Jonsson, and Kew*). See Pet., p. 1. Accordingly, there has been “road-mapping” with respect to at least the BOA IPR. This factor favors denying institution.

4. General Plastic Factors Four and Five

Petitioner knew or should have known about the prior art asserted in the Petition (*Veneklase, Jonsson, Kew, Sormunen, and Kaufman*) shortly after being served with the complaint (i.e., February 2023). See Pet., p. 8. That is because Petitioner was served the complaint less than two months after the BOA IPR and the

Unified IPR were filed, and as discussed above, all the references relied upon in the instant Petition were at least cited in the BOA IPR and/or the Unified IPR.

The institution decisions in the BOA IPR and the Unified IPR were issued nearly five months after Petitioner was served with the complaint (i.e., July 2023). Petitioner then waited an additional five months after those decisions—a total of ten months after service of the complaint—to take a fourth bite at the apple, filing the instant Petition on December 18, 2023. Accordingly, Petitioner waited approximately ten months to file the Petition after learning about the prior art. Further, the Petition provides no explanation for this ten-month delay. In *Valve Corp. v. Electronic Scripting Products, Inc.*, the Board found that a five-month delay was sufficient to favor denying institution. *Valve Corp. v. Electronic Scripting Products, Inc.*, IPR2019-00064, Paper 10 at 15 (P.T.A.B. May 1, 2019) (precedential) (“The fact that Valve waited five months after HTC’s petition to file the Petition in this case favors denying institution.”). These factors favor denying institution.

5. General Plastic Factor Six and Seven

The instant Petition uses the institution decisions in the BOA IPR and the Unified IPR as roadmaps, presenting prior art and arguments that have already been considered by the Office. The overlap in the challenged claims and the significant

relationship between Petitioner and the petitioners of the Unified IPR and BOA IPR favors denying institution because this Petition would be redundant and a waste of the Board's finite resources. *See Valve Corporation v. Electronic Scripting Products, Inc.*, IPR2019-00062, Paper 11 at 15 (P.T.A.B. April 2, 2019) (precedential) ("Here, [Petitioner] waited until after the institution decision[s] in the [Unified and BOA] IPR[s], and then filed . . . [an] additional petition[]. These serial and repetitive attacks implicate the efficiency concerns underpinning *General Plastic*, and, thus, favor denying institution."). Thus, the sixth and seventh *General Plastic* factors therefore favor denying institution.

The *General Plastic* factors overwhelmingly favor denying institution.

IV. THE PETITION SHOULD BE DENIED BECAUSE IT DOES NOT ESTABLISH A REASONABLE LIKELIHOOD OF SUCCESS ON ANY CHALLENGED CLAIM

As shown below, the Petition fails to demonstrate a reasonable likelihood that Petitioner would prevail with respect to either of the Challenged Claims. As detailed herein, the proposed Grounds fail to disclose key limitations of each Challenged Claim, so trial should not be instituted.

A. 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.

EX1001. 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.” EX1001 at 1:7-11.

At the time of the claimed inventions, “secure systems”² 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.

²The '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.” EX1001, 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.”

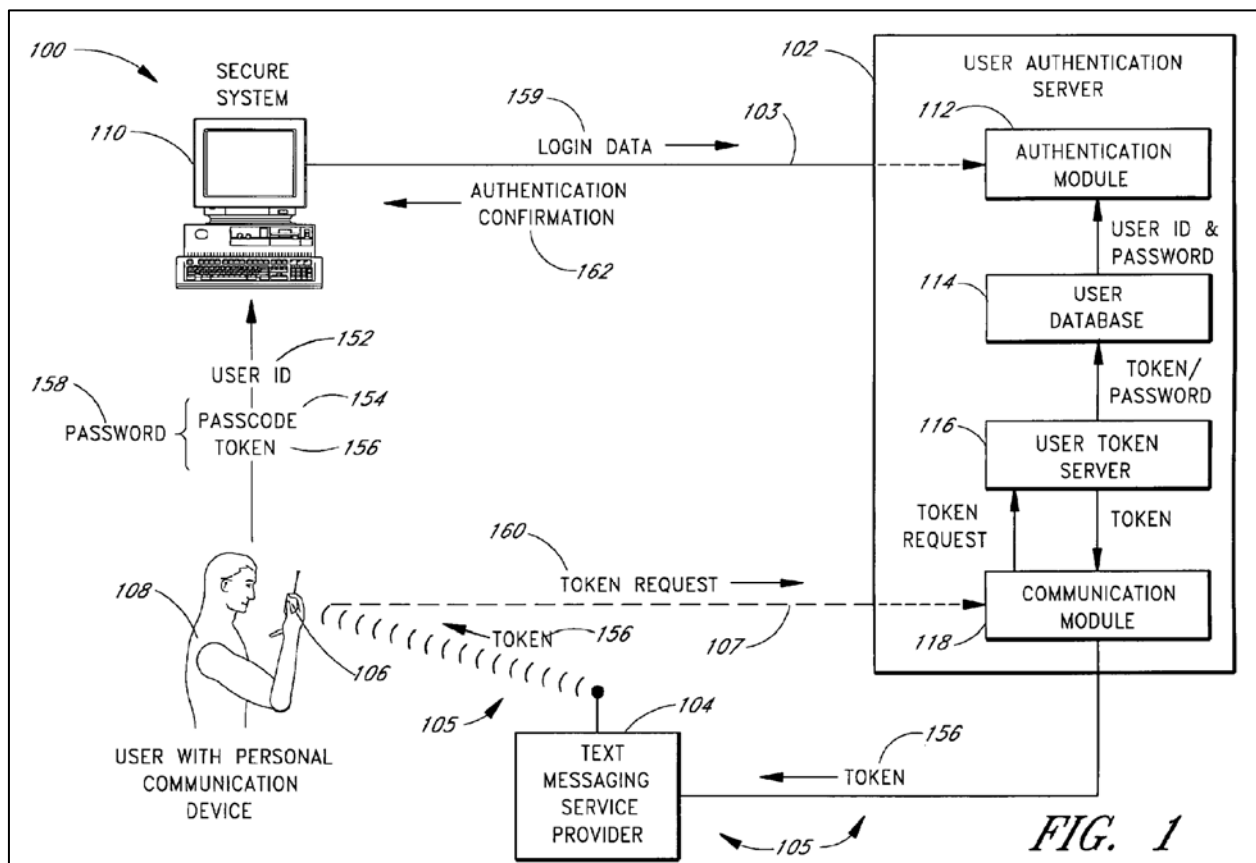
Id. at 2:11-15.

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):



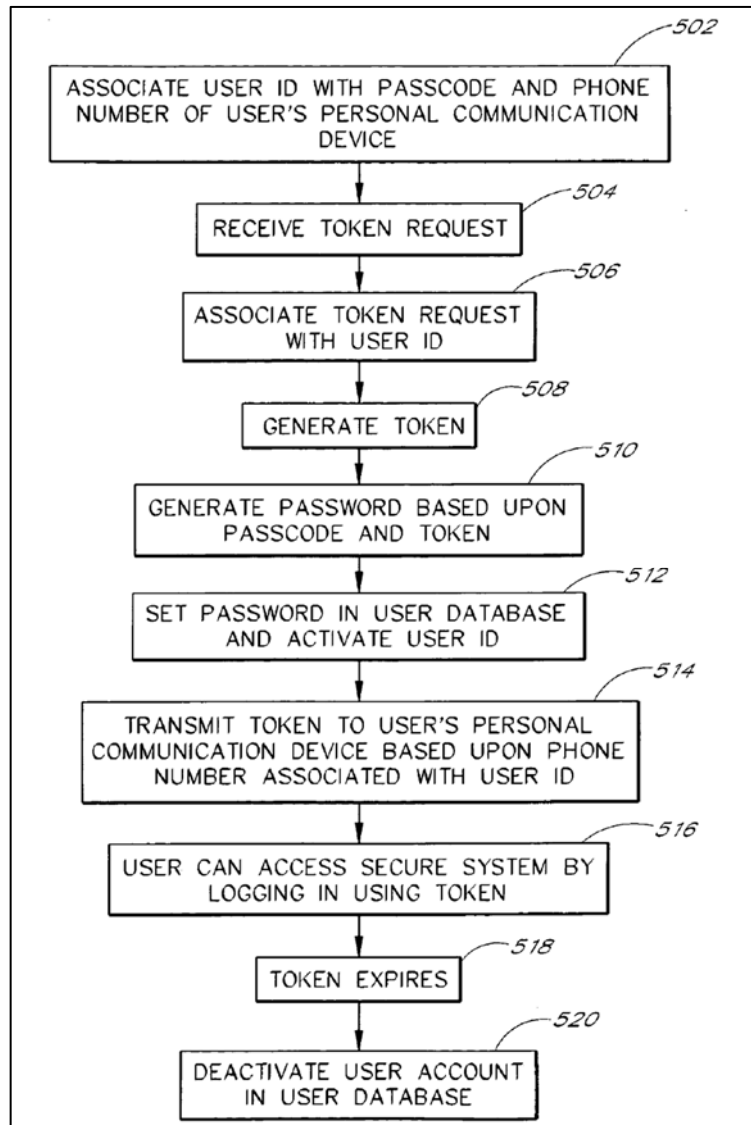
EX1001 at Fig. 1; *see also id.* at 3:31-33.

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 specification discloses that, in some embodiments, the “predetermined amount of time” can be stored in a user database. *See id.* at 8:20-28.

The Patent Office issued the ’658 Patent issued after multiple office actions. Since then, the ’658 Patent has been cited by more than 200 patent applications.

EX2005, <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.*

B. Level of Ordinary Skill in the Art

For the purposes of this Response only, Patent Owner does not dispute the level of skill of a person of ordinary skill in the art (“POSITA”) identified in the Petition. *See Pet.*, pp. 14-15. Patent Owner notes, however, that the United States District Court for the Eastern District of Texas found that a POSITA would have at least an undergraduate degree in electrical engineering, computer science, computer engineering, or a closely related field, and two years experience in online security, such as user authentication technologies. EX1011 at 6-7.

C. Claim Construction

Petitioner has correctly identified Judge Payne’s constructions in *Dynapass IP Holdings LLC v. JPMorgan Chase & Co.*, Case No. 2:22-cv-00212-JRG-RSP (E.D. Tex.). *See Pet.* at 15. The Board is required to apply the same claim-construction standard as in Federal district court. 37 C.F.R. § 42.100(b). Although

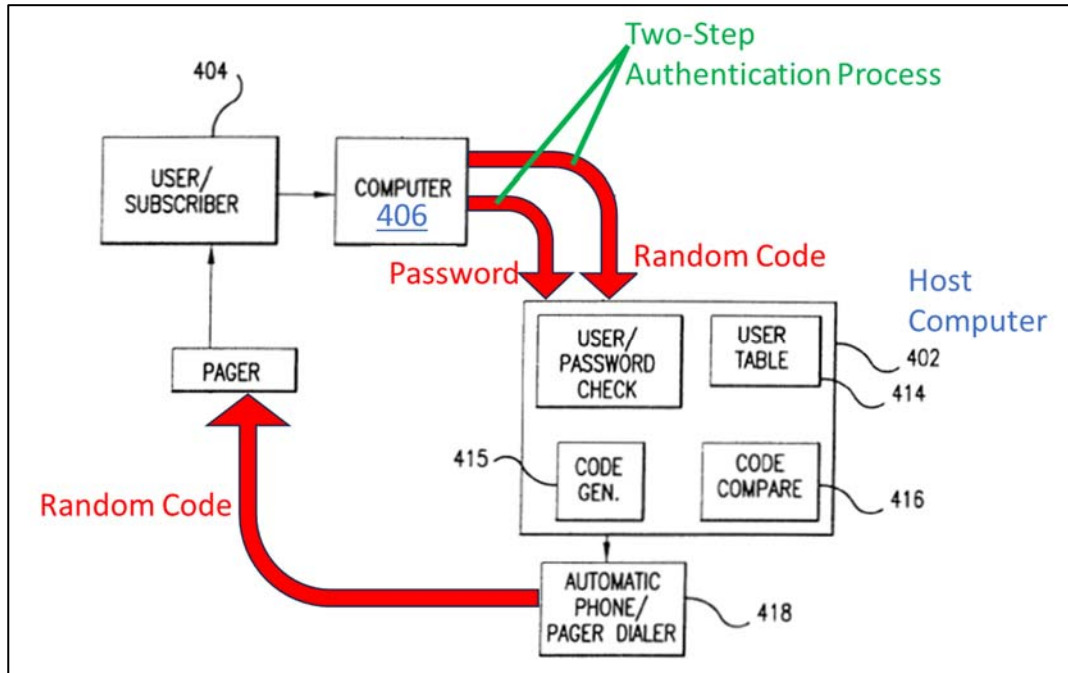
Patent Owner disputes certain constructions from the district court, Patent Owner respectfully requests that the Board apply those constructions here.

In particular, the court construed the term “activating access to the account in response to the password,” as recited by claim 5, to mean “activates access to the account in response to the creation of the password.” EX1011, p. 16. Petitioner asserts “[f]or the purposes of this proceeding . . . this [term] should be construed according to the District Court’s construction.” Pet., p. 32 n.9. Patent Owner agrees.

Patent Owner reserves the right to address claim construction of any term in the challenged claims if the Board institutes *inter partes* proceedings.

D. Cited Art

Veneklase discloses a computer security system including a user’s “computer 406,” a user’s “pager 420,” and a “host computer 402.” EX1005, 7:29-51, Fig. 6. Figure 6 of *Veneklase* is reproduced below:

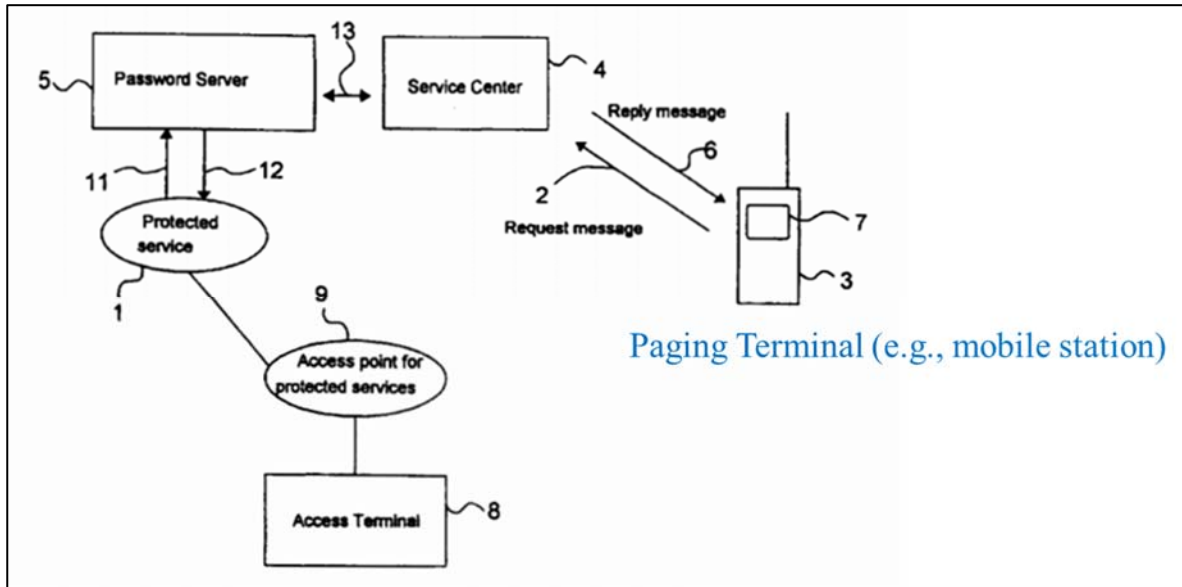


EX1005, Fig. 6 (excerpted and annotated). During an authentication process, the user transmits a “password” from “computer 406” to “host computer 402.” EX1005, 7:58-8:27. “Host computer 402” then “cross references the received password [] against a pager phone number list” stored within “host computer 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 retrieved pager number. *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. *See id.*, 7:16-28.

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.” EX1007, 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.

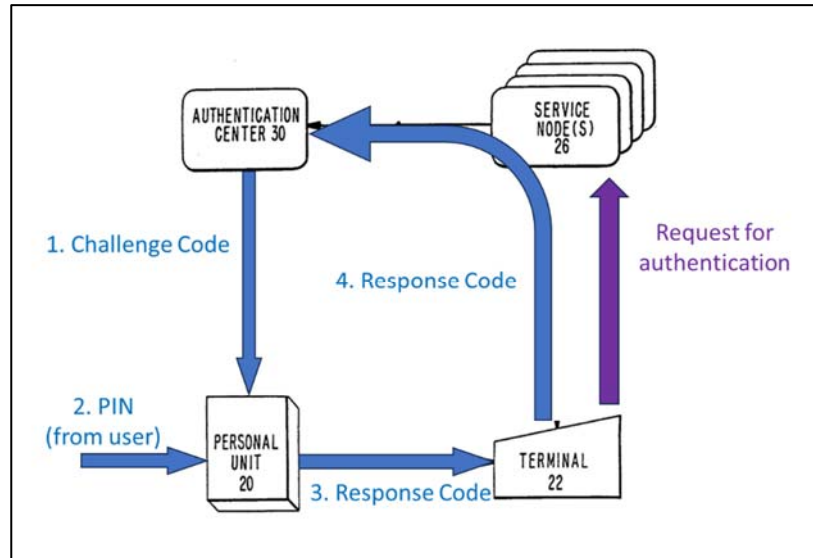


EX1007, Fig. 2 (annotated). The “short message 2 includes a password request.” *Id.*, 5:38-6:1. Then, the “paging service center 4 processes the incoming message and forms according to it a data transmission connection to a password server 5 and transmits the inquiry to it,” which “processes the message and forms a reply message containing one or more passwords.” *Id.*, 6:20-24. Finally, “the reply message 6 [received by] 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.” *Id.*, 7:4-7.

But *Veneklase* and *Sormunen* each fail to disclose generating a “password” based on a “token” and “passcode,” as the challenged claims require. Further, *Veneklase* and *Sormunen* fail to disclose deactivating an account “within a predetermined amount of time after activating the account,” as the challenged claims

require. Further still, *Veneklase* and *Sormunen* fail to disclose using the same cell phone network to both receive a request for the token from the personal communication device and transmit the token to the personal communication device, as the challenged claims require.

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 EX1006, 9:1-10:2, Fig. 1. Figure 1 of *Jonsson* is reproduced below:



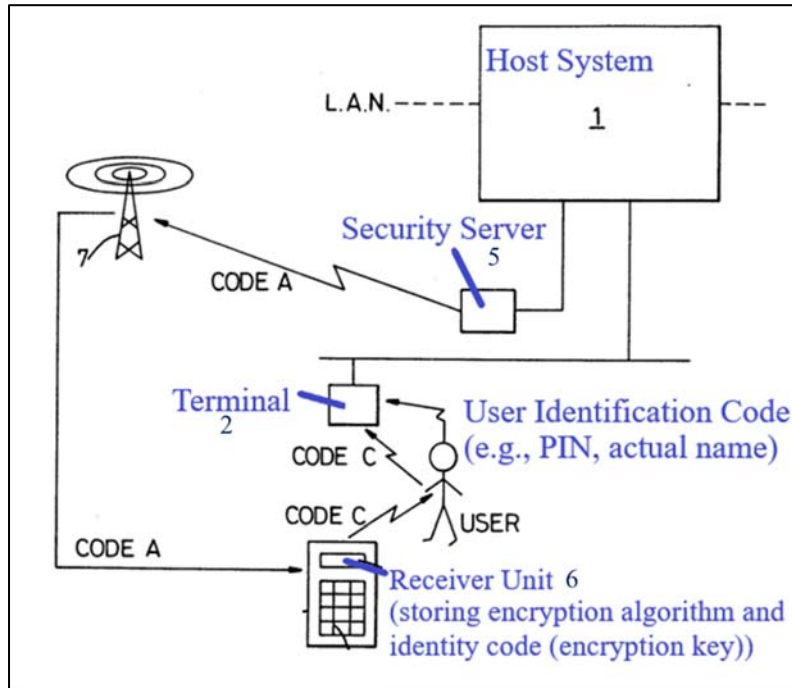
EX1006, Fig. 1 (annotated). Following a request for authentication, *Jonsson*’s “authentication center 30” generates a “challenge code” and sends the “challenge code” to the “personal unit 20.” EX1006, 9:1-7. When the “personal unit 20” receives the “challenge code,” it “prompts the user to input a PIN” and “generates a response code” using a stored algorithm that utilizes the PIN as an input. *Id.*, 9:9-

25. 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.*

Kaufman is discussed above in Section III.A.

But *Jonsson* and *Kaufman* each fail to disclose deactivating an account “within a predetermined amount of time after activating the account,” as the challenged claims require. Further, *Jonsson* and *Kaufman* fail to disclose using the same cell phone network to both receive a request for the token from the personal communication device and transmit the token to the personal communication device, as the challenged claims require.

Kew discloses a computer security system including a “host system 1,” a “security server 5,” a “receiver unit 6,” and a “remote terminal 2.” EX1009, 7:34-9:11, Fig. 1. Figure 1 of *Kew* is reproduced below:



Id., 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.” *Id.*, 7:20-32.

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 id.*, 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 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.*

But *Kew* fails to disclose deactivating an account “within a predetermined amount of time after activating the account,” as the challenged claims require. Further, *Kew* fails to disclose using the same cell phone network to both receive a request for the token from the personal communication device and transmit the token to the personal communication device, as the challenged claims require. Further still, *Kew* fails to disclose that the “token” is eventually known to the user and that the “passcode” is known to the user, as the challenged claims require.

E. Ground 1 – The Combination of *Veneklase*, *Jonsson*, and *Sormunen* Does Not Render Obvious Dependent Claim 7.

Dependent claim 7 depends from claim 6, which depends from claim 5. Accordingly, dependent claim 7 has all the requirements of claims 5 and 6. 35 U.S.C. § 112, ¶4. The Petition’s defects regarding claims 5 and 6 are discussed before the defects specific to claim 7.

1. Independent Claim 5

The combination of *Veneklase* and *Jonsson* does not teach or suggest the following claim elements. Petitioner does not rely on *Sormunen* to teach or suggest any element of claim 5. *See* Pet., pp. 16-39.

- i. 5[c] “a control module . . . configured to create a new password based at least upon a token and a passcode”

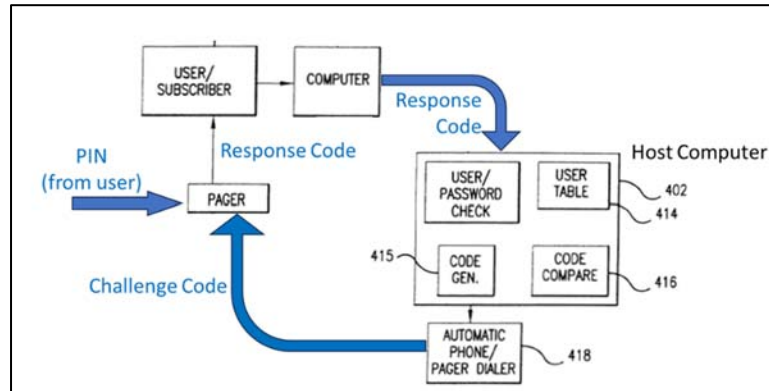
Petitioner mapped *Veneklase*’s “user/password check” module to the claimed “control module” (*see* Pet., pp. 23-24), but concedes that *Veneklase* does not disclose this claim element. *See* Pet., p. 24. Petitioner argues that the combined teachings of *Veneklase* and *Jonsson* meet the requirements of claim element 5[c]. *See* Pet., pp. 22-26. But Petitioner’s proposed combination fails to support a conclusion of obviousness for multiple reasons.

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 36 (citing EX1005, 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).

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 EX1006, 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.

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., pp. 24-25, 36, and 39. *Veneklase*’s modified system is depicted below:



EX1005, Fig. 6 (excepted and annotated).

But modifying *Veneklas*'s system by eliminating the two-step authentication process, as proposed by Petitioner, changes *Veneklas*'s principle of operation. *Veneklas*'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." EX1005, 7:16-28. Accordingly, this two-step authentication process is a key feature of *Veneklas*'s principle of operation, and a POSITA would not seek to remove steps as Petitioner proposes. 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.").

Petitioner also argues that

a POSITA would have been motivated to combine *Veneklase* and *Jonsson* because implementing the algorithm of *Jonsson*'s system in *Veneklase*'s authentication system provides an additional layer of security. For example, a POSITA would have understood that implementing *Jonsson*'s algorithm system would prevent unauthorized personnel from being able to access the system by engaging in SIM swapping.

Pet., p. 37 (emphasis added). But *Veneklase*'s two-step authentication process already “allows for multiple levels of security before access to the computer system is achieved.” EX1005, 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.” EX1005, 8:2-5. Petitioner concedes as much. See Pet., p. 33 (“*Veneklase* discloses that this system is accessible only when the password is found within the master password list.”) (emphasis added). *Veneklase* identifies the two-step process as providing an additional 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 EX1005, 7:16-21.

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. Neither Petitioner nor its expert provides any evidence that the security of the proposed combination is superior to the existing multi-layer/level security in *Veneklase*. See Pet., pp. 35-39; EX1002, ¶¶101-108.

As for SIM swapping, it would also not work in *Veneklase's* existing system because the hackers would still need *Veneklase's* password. Further, as discussed below regarding claim element 5[d], the combined system would be more prone to Denial of Service (DoS) attacks by hackers. 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*.

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 *Jonsson's*, because it explicitly discloses embodiments in which data streams are encoded and decoded using algorithms for additional security.” Pet., p. 37 (citing EX1005, 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.

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].” EX1005, 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.” EX1005, 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*].” EX1006, 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. 37.

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

- ii. 5[d] “a communication module configured to transmit the token to the personal communication device through the cell phone network”

Petitioner argues that this claim element is met by the “automatic phone/pager dialer 418” in *Veneklase*. Pet., p. 27. Petitioner’s argument is contrary to its own modifications to *Veneklase* that were necessary to allegedly meet the requirements of claim element 5[c].

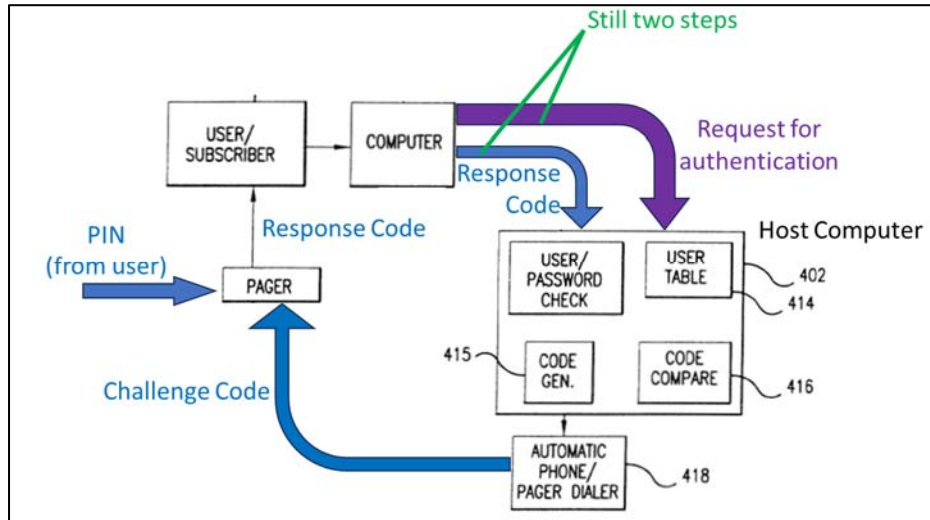
Veneklase’s system (1) receives the password from the user (step one in the two-step authentication process), (2) uses the received password to lookup the phone number associated with the user, (3) generates a random code, (4) transmits the random code to the user’s pager using the phone number identified from the received password, and then (5) receives the random code from the user (step two in the two-step authentication process). See EX1005, 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.*

As discussed above in reference to claim element 5[c], 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 eliminated 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. 33 ("*Veneklase* discloses that this system is accessible only when the password is found within the master password list.") (emphasis added). Neither Petitioner nor its expert explain 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). See Pet., pp. 26-28; EX1002, ¶¶88-92. 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, 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). That is a fatal defect in the Petition.

If Petitioner is arguing that the user’s device would be identified through an authorization request, as disclosed in *Jonsson*, that position is also flawed. As discussed above regarding claim element 5[c], Petitioner’s motivation for combining *Veneklase* and *Jonsson* includes “reducing what needs to be entered through the secure computer network to a single step (i.e., single entry of the generated response code) in order to simplify the process and save time.” Pet., p. 36 (emphasis added). 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 requires multiple steps where things are entered and transmitted through the secure computer network: (1) a first step where the user’s “authentication request” is entered/transmitted through the secure computer network to trigger generation of a “challenge code” (EX1006, 9:1-4, 10:18-20, Fig. 3), and then (2) a second step where the “response code” is entered/transmitted through the secure computer network for a comparison with the expected response code (EX1006, 9:26-30, 11:4-13, Fig. 3). That scenario is depicted below:



EX1005, Fig. 6 (excepted and annotation). Thus, Petitioner’s rationale for combining *Veneklase* and *Jonsson* is not actually realized (i.e., multiple transmissions through secure computer network still remain after the modification), and a POSITA would not be motivated to execute the proposed combination.

According to Petitioner, a “POSITA would have been motivated to combine *Veneklase* and *Jonsson* because having only one password transmitted via computer system is more efficient and secure.” Pet., p. 36 (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), in which case the proposed combination is open to Denial of Service attacks (DoS). Specifically, nothing prevents a hacker from continuously transmitting the non-secret “authentication request” to the system, triggering generation and transmission of “challenge codes” to the legitimate user’s

“personal communication unit” (e.g., pager)—thus interfering with the legitimate user’s access to the system. That is a denial of service (DoS) attack. *See* EX2007, 1:14-16 (“A ‘denial of service’ (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.”). In contrast, *Veneklase*’s existing system requires a password (i.e., a secret) to trigger generation and transmission of the “random number code” to the legitimate user’s “pager 420.” *See* EX1005, 8:1-15. Accordingly, the aforementioned DoS attack is less likely with *Veneklase*’s system.

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

- iii. 5[e] “an authentication module configured to receive the password from the user through a secure computer network”

Claim 5 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[e] *with* claim element 5[c]. Petitioner argues that “*Veneklase*, alone or in combination with *Jonsson*, teaches this limitation.” Pet., p. 28 (emphasis added). Patent Owner disagrees.

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. 24 (*Veneklase* “does not disclose creating a new password based on those two items.”).

Further, 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.” EX1006, 8:12-14. *Veneklase* discloses its “invention is very cost effective as it employs substantially ‘off the shelf’ and readily available components.” EX1005, 7:22-24. Indeed, *Veneklase*’s “pager 420” only needs to be capable of receiving a message and displaying the message (i.e., intrinsic functions of an off-the-shelf pager) to be ready for use in *Veneklase*’s system. But neither Petitioner nor its expert provide any evidence that an off-the-shelf pager, in 1996, was capable of executing *Jonsson*’s specialized security algorithms without heavy software/hardware customization. *See* Pet., pp. 28-31; EX1002, ¶¶88-92. In fact, *Jonsson* expressly states that its algorithm requires a highly specialized “personal unit,” not just an off-the-shelf pager. *See* EX1006, 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).

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

- iv. 5[f] “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”

As discussed above in Section IV.C, the United States District Court for the Eastern District of Texas construed the term “activating access to the account in response to the password” to mean “activates access to the account in response to the creation of the password.” EX1011, p. 16. Petitioner asserts “[f]or the purposes of this proceeding . . . [that term] should be construed according to the District Court’s construction.” Pet., p. 32 n.9. Patent Owner agrees.

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:

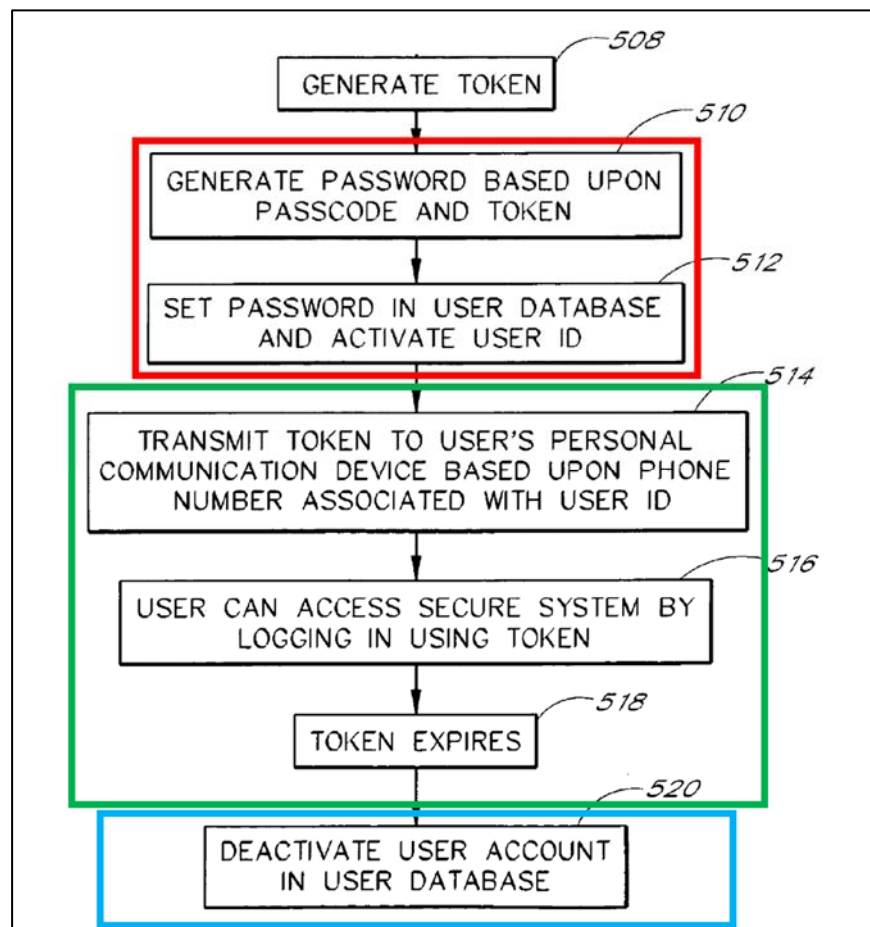
a control module executed on the computer processor configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a password associated with the user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

EX1001, 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.*, 12:27-33. The “authentication module” claim element recites “the password” several times. *See id.*, 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.*, 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.”

Also based on the claim language, “activating access to the account” starts a “predetermined amount of time,” and the “authentication module” deactivates the account upon expiration of the “predetermined amount of time.” EX1001, 12:41-45. The “predetermined amount of time” corresponds to the entire time period between activation and deactivation of the account. *See id.* That process is depicted, for example, in Figure 5, which is reproduced in pertinent part below:



EX1001, 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 of the account occurs in step 520 (as highlighted in blue in Figure 5). *See id.* at 9:61-64, Fig. 5. The “predetermined period of time” is the entire time period between those two events (as highlighted in green in Figure 5). *See id.* at 12:41-47, Fig. 5.

Petitioner mapped *Veneklase*’s “predetermined period of time” to the claimed “predetermined amount of time,” but that mapping is flawed. *See Pet.*, pp. 33-35. Specifically, *Veneklase*’s “predetermined period of time” starts when *Veneklase*’s system receives the password (also called the “first password”) from the user (i.e., step one in *Veneklase*’s two-step authentication process). *See EX1005*, 8:40-49. *Veneklase*’s token (also called the “second password”) must be received (i.e., step two in *Veneklase*’s two-step authentication process) before the “predetermined period of time” expires. *See id.* In contrast, as discussed above, the claimed “predetermined amount of time” starts with activation of access to the account in response to creation of a password, by the system, based on a passcode and a token.

Further, to meet the requirements of claim element 5[c] (discussed above), Petitioner’s modification eliminated step one in *Veneklase*’s two-step authentication process where the system receives the password (i.e., “first password”) from the user. *See Pet.*, pp. 24-25, 36, 39. But with that first step eliminated, *Veneklase*’s

system would not receive the user's password (i.e., "first password"), and thus *Veneklase's* "predetermined period of time" would not even start.

The flaws in Petitioner's mappings do not end there. According to Petitioner,

The "timing means 40 records the time at which the first and second passwords are received by analyzing means 12" and "then compares the times to determine whether the second password [sent to the cellular phone] was received **within a predetermined period** or predetermined 'window' of time after the first password [i.e., the expected response code] was received," which corresponds to the time at which it was created and activated the account.

Pet., pp. 33-34 (emphasis added). That is misleading and simply wrong. *Jonsson's* "expected response code" is generated by the system—it is never received from the user (the user sends the "response code," not the "expected response code"). See EX1006, 9:26-10:5 (the received "response code is compared to an expected response code"). Accordingly, *Jonsson's* "expected response code" cannot be compared to *Veneklase's* "first password" or even "second password."

Further, in the *Veneklase-Jonsson* system, the only thing "sent to the cellular phone" is the "challenge code." See EX1006, 9:9-13. But the *Veneklase-Jonsson* system never receives the "challenge code" from the user. See *id.* Accordingly, the "challenge code" cannot be compared to *Veneklase's* "second password" or even "first password."

According to Petitioner,

The predetermined period would thus be the time allowed after generation of the expected response code [by the system] and/or of the new password [i.e., response code] by the personal communication device (which a POSITA would have understood occur at or around the same time) for the user to enter and send the new password to computer 402.

Pet., pp. 34-35 (emphasis added). That is simply wrong. Again, *Veneklase's* “predetermined period of time” starts when *Veneklase's* system receives the password (i.e., “first password”) from the user (i.e., step one in *Veneklase's* two-step authentication process), a step that was eliminated with Petitioner’s modifications to *Veneklase*.

Even if the “predetermined period of time” in the *Veneklase-Jonsson* system started with generation of response code by the user’s cellphone/pager, it still would not meet the requirements of claim element 5[f]. Specifically, the cellphone/pager must wait for the user to enter the PIN before the cellphone/pager can generate the response code. *See* EX1006, 9:9-13. Thus, *Veneklase's* “code compare module 416” (Petitioner-identified “authentication module”) has no way of knowing when the “predetermined amount of time” started, no way of knowing when the “predetermined amount of time” ends, and thus no way of knowing when to deactivate the account, as claim 5 requires.

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

2. Dependent Claim 6

Claim 6 recites “wherein the communication module is further configured to receive a request from the user for the token, and wherein the control module is further configured to create the new password in response to the request.” EX1001, 12:48-52. The combination of *Veneklase* and *Jonsson* does not render claim 6 obvious. Petitioner does not rely on *Sormunen* to teach or suggest claim 6. *See* Pet., pp. 39-41.

As a threshold matter, claim 6 depends from and adds limitations to independent claim 5. The combination of *Veneklase* and *Jonsson* fails to render claim 5 unpatentable, therefore, the combination of *Veneklase* and *Jonsson* also fails to render claim 6 unpatentable for at least the same reasons.

Further, Petitioner mapped *Veneklase*’s “automatic phone/pager dialer 418” and the user’s submission of the password through the first communication channel to the claimed “communication module” and claimed “request . . . for the token,” respectively. *See* Pet., pp. 27 (“A POSITA would have recognized that *Veneklase*’s automatic phone/pager [dialer 418] discloses the claimed communication module”), 40 (“a POSITA would have understood that the user’s submission of the password through the first communications channel is a request from the user for the token.”). Those mapping are flawed.

First, Petitioner provides zero evidence that *Veneklase*'s "automatic phone/pager dialer" (Petitioner-identified "communication module") receives the user's submission of the password through the first communication channel (Petitioner-identified "request . . . for the token"), as claim 6 requires. *Veneklase* is silent regarding the "automatic phone/pager dialer" receiving anything from the user, and there is no evidence that the "automatic phone/pager dialer" can even access the first communication channel. EX1005, Fig. 6. In fact, *Veneklase* discloses it is the "host computer 402," not the "automatic phone/pager dialer," that receives the user's submission of the password. *See id.*, 8:1-3 ("host computer 402 . . . cross references the received password"). *Veneklase* also discloses the "automatic phone/pager dialer" communicates via the "second communication channel 422," not the "first communication channel 412." *See id.*, 8:11-15, Fig. 6. Those are fatal defects in the Petition.

In one instance, Petitioner mapped *Veneklase*'s "user/password check module" to the claimed "communication module." *See Pet.*, p. 41 ("*Veneklase* . . . teaches wherein the communication module (e.g., user/password check module)"). But Petitioner concedes that *Veneklase*'s "user/password check module" (Petitioner-identified "communication module") does not "transmit the token to the personal communication device through the cell phone network," as claim 6 requires by virtue

of its dependency from claim 5. *See* Pet., p. 27. At bottom neither *Veneklase's* “user/password check module” nor *Veneklase's* “automatic phone/pager dialer” meets all the requirements of the “communication module” recited by claim 6.

Second, to meet the requirements of claim element 5[c] (discussed above), Petitioner modified *Veneklase* by eliminating the step where the user submits the password to the host system through the first communication channel (i.e., eliminated step one of *Veneklase's* two-step authentication process). *See* Pet., pp. 24-25, 36, 39. But now Petitioner is relying on the eliminated step to meet the requirements of claim 6. That is a fatal defect in the Petition.

3. Dependent Claim 7

Claim 7 recites “wherein the request [for the token] is transmitted by the user through the personal communication device.” Ex.1001, 12:53-55. *Veneklase* discloses that the initial submission of a password (Petitioner-identified “request . . . for the token”) is performed using a “first communications channel,” while transmission of *Veneklase's* “random code” to the user’s cellphone/pager (Petitioner-identified “transmit the token to the personal communication device”) is performed using a “second communications channel.” *See* EX1005, 6:5-37, Figs. 1, 2, 6. The first and second communication channels are

two distinct communications channels . . . in order to ensure 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 . . . Further, the use of a “secret” password, a “secret” substantially random number, and a “secret” second channel allows for multiple levels of security before access to the computer system is achieved and provides enhanced security over the prior art.

Id., 7:16-28 (emphasis added). *See also id.*, Abstract, 3:50-4:15, 6:5-37, 7:39-8:15.

In other words, the use of two distinct communication channels is part of *Veneklase*’s security architecture that distinguishes it from the prior art and thus a key feature in *Veneklase*’s principle of operation.

Petitioner proposes modifying *Veneklase* such that the user’s submission of the password (Petitioner-identified “request . . . for the token”) and transmission of the random code (Petitioner-identified “transmit the token to the personal communication device”) are both accomplished using *Veneklase*’s “communication channel 422” (Petitioner-identified “cell phone network”), as allegedly disclosed by *Sormunen*. *See* Pet., pp. 20, 42-43. But that modification dismantles *Veneklase*’s security architecture and thus changes *Veneklase*’s principle of operation. Accordingly, the proposed modification to *Veneklase* is too drastic to be obvious.

Petitioner argues a POSITA would have modified *Veneklase* based on *Sormunen* because “the system in *Veneklase* would also benefit from the fast data speeds and security offered by widely deployed communications networks to allow for secure access to a service ‘almost immediately’ after a request is sent. *See*

EX1007, 5:12-18 (“[a] further advantage of the fast data transmission is that...security may thus be improved”).” Pet., p. 45 (emphasis added). But neither Petitioner nor its expert offer any evidence that *Veneklase*’s modified system would be faster or more secure than *Veneklase*’s original system. See Pet., p. 45; EX1002, ¶125. *Sormunen*’s use of “very fast” and “almost immediately” is a comparison with older systems that utilize the postal service or that require a human review for a subscription request. See EX1007, 3:6-4:16. But *Veneklase* is not one of those older systems.

Further, the alleged security in *Sormunen* arises from transmission of sensitive data from the system to the user’s cellphone/pager. See EX1007, 4:18-24 (“An object of the present invention is to eliminate the disadvantages disclosed above and to establish a method wherein transmission of user specific authentication data from the service provider to the user of the service can be performed as fast and as safely as possible. The invention is based on the idea that user specific authentication data is transmitted to the user by using, at least partly, a paging system or a short message service.”) (emphasis added). Again, *Veneklase*’s original system already transmits sensitive data (i.e., the token) to the user’s cellphone or pager. See EX1005, 8:56-57 (“communications channel 84 comprises a pager or cellular phone”). Accordingly, there is no motivation to modify *Veneklase* based on *Sormunen*.

According to Petitioner,

a POSITA would have recognized that this combination would offer increased security over the *Veneklase-Jonsson* system by ensuring that tokens are only sent to devices already in the hands of the user at the time of the request, rather than to a device that may have been misplaced or even lost.

Pet., p. 46 (emphasis added). Petitioner is misguided. If the user has misplaced or lost their device (e.g., cellphone), the user would not even contemplate using the *Veneklase-Jonsson* system knowing that the required token would be sent to the misplaced/lost device. Accordingly, the alleged “increased security” resulting from the combination with *Sormunen* is non-existent.

F. Ground 2 – The Combination of *Veneklase*, *Jonsson*, *Sormunen*, and *Kaufman* Does Not Render Obvious Dependent Claim 2.

Claim 2 depends from claim 1. Accordingly, claim 2 has all the requirements of claim 1. 35 U.S.C. § 112, ¶4. The Petition’s defects regarding claim 1 are discussed before the defects specific to claim 2.

1. Independent Claim 1

As a threshold matter, Petitioner does not rely on *Kaufman* to teach or suggest any element of claim 1. See Pet., p. 48. Further, Petitioner argues “claim 1 recites limitations analogous in scope to those of claim 5.” *Id.* As discussed above, the combination of *Veneklase* and *Jonsson* fails to teach or suggest claim elements 5[c], 5[d], 5[e], and 5[f]. Accordingly, the combination also fails to teach or suggest the

corresponding claim elements in independent claim 1. Petitioner argues that claim element 1[b] is analogous to claim 7. *See id.* As discussed above, the combination of *Veneklase*, *Jonsson*, and *Sormunen* fails to render obvious claim 7, and thus also fails to render obvious claim element 1[b].

2. Dependent Claim 2

As a threshold matter, the combination of *Veneklase*, *Jonsson*, and *Sormunen* fails to render claim 1 unpatentable (discussed above). *Kaufman* does not cure the deficiencies of *Veneklase*, *Jonsson*, and *Sormunen* regarding claim 1, and the Petition does not assert otherwise. *See* Pet., pp. 50-55. Accordingly, the combination of *Veneklase*, *Jonsson*, *Sormunen*, and *Kaufman* fails to render claim 1 unpatentable. Claim 2 depends from and adds limitations to claim 1. Thus, the combination of *Veneklase*, *Jonsson*, *Sormunen*, and *Kaufman* fails to render claim 2 unpatentable for at least the same reasons.

Further, *Kaufman*'s "authentication token generator" is similar to RSA's SecurID product disclosed in the '658 Patent. *See* EX1001, 1:44-59. Both *Kaufman*'s "authentication token generator" and RSA's SecurID product are additional devices (i.e., not the user's cellphone, not the user's pager) that the user must carry with him/her and that locally generate one-time access codes based on time, without receiving the token. *Compare* EX1008, 8:55-60, 9:30-36 *with*

EX1001, 1:44-59. And they continually generate one-time access codes without irrespective of whether the user requests one. *Compare* EX1008, 9:31-36 with EX1001, 1:49-51. But the '658 Patent expressly discloses the claimed invention is designed to operate with the user's personal communication device to save the user from having to carry around yet another device like RSA's SecurID product or *Kaufman's* "authentication token generator." *See* EX1001, 1:56-59 ("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.") (emphasis added). Accordingly, *Kaufman* with its necessary "authentication token generator" teaches away from the claimed invention and cannot render the claimed invention obvious. "Obviousness may be defeated if the prior art . . . teaches away from the invention. A reference teaches away when a person of ordinary skill, upon reading the reference . . . would be led in a direction divergent from the path that was taken in the claim." *Meiresonne v. Google, Inc.*, 849 F.3d 1379, 1382 (Fed. Cir. 2017) (cleaned up). The Petition is effectively taking the same prior art (i.e., RSA's SecurID product) and recasting it through impermissible hindsight.

According to Petitioner, a "POSITA who is looking to maximize the benefits of *Veneklase's* invention would have been motivated to implement *Kaufman's*

disclosed concatenation and ‘cryptographically secure hashing algorithm’ (EX1008, 7:2-5) in order to add an additional layer of security.” Pet., p. 54 (emphasis added). But neither Petitioner nor its expert provide any evidence that the “benefits of *Veneklase*’s invention” have not already been “maximized” through use of *Jonsson*’s algorithm (e.g., GSM 03.20, Appendix C.2, algorithm A3). See EX1006, 7:11-12; Pet., pp. 52-55, EX1002, ¶¶147-148. Similarly, neither Petitioner nor its expert provide any evidence that *Kaufman*’s algorithm is superior to *Jonsson*’s algorithm with respect to “add[ing] an additional layer of security.” See *id.*

Further, Petitioner argued that “a POSITA would have been motivated to utilize the ‘hashing algorithm’ in *Kaufman* in the system of *Veneklase* because it would have a simple replacement [*sic*] or additional process that would have been applied to generating *Veneklase*’s ‘random number code.’” Pet., p. 54 (emphasis added). But Petitioner is not applying *Kaufman*’s algorithm to generate *Veneklase*’s “random number code” (or *Jonsson*’s “challenge code”); it is being applied to generate *Jonsson*’s “response code.” See Pet., p. 52.

Accordingly, Petitioner has not shown there is a motivation to combine *Kaufman* with *Veneklase* and *Jonsson*.

G. Ground 3 – The Combination of *Kew* and *Sormunen* Does Not Render Obvious Dependent Claim 7.

Dependent claim 7 depends from claim 6, which depends from claim 5. Accordingly, dependent claim 7 has all the requirements of claims 5 and 6. 35 U.S.C. § 112, ¶4. The Petition’s defects regarding claim 5 are discussed before the defects specific to claim 7.

1. Independent Claim 5

The combination of *Kew* and *Sormunen* does not teach or suggest the following claim elements.

- i. 5[c] “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”

Petitioner mapped *Kew*’s “security server,” “Code A,” and “identity code” to the claimed “control module,” “token,” and “passcode,” respectively. *See* Pet., p. 64. Those mappings are flawed for multiple reasons.

First, the claim language is unequivocal: “the passcode is known to the user.” EX1001, 12:29-32. *Kew*’s “identity code” is not the claimed “passcode” because it is not known to the user. *Kew*’s “identity code is [an encryption] 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.”

EX1009, 7:29-32 (emphasis added). The “identity code” is stored in the EPROM of receiver unit 6. *Id.*, 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 id.*, 8:33-36 (emphasis added). That is why *Kew* contains no disclosure of the user knowing the “identity code.”

Moreover, a POSITA would understand that the “identity code” would not be known to the user, as claim 5 requires. 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. EX2008, p. 195. They are “reprogrammed by removing the protective cover from the top of the chip and exposing the chip to ultraviolet light.” *Id.* The choice in *Kew* to store the “identity code” in EPROM, as opposed to RAM, indicates that the “identity code” is not input to receiver unit 6 by the user; rather the device is pre-programmed with the “identity code.” 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 would understand that the “identity code” would not be known to the user, contrary to what claim element 5[c] requires.

In an attempt at sleight of hand, the Petition misleadingly confounds the “identity code” and the “user identification code:”

The user’s identity

code, on the other hand, “should preferably be treated by the user as a secret code” and “is thus comparable with a personal identification number (PIN),” and is therefore known to the user beforehand. *Id.*, 3:8-12, 7:36-8:2; Ex.1002, ¶166.

See Pet., p. 63. Here is what *Kew* actually says, without Petitioner’s fabrication:

The user identification code should preferably be treated by the user as a secret code and not be marked on the receiver. It is thus comparable with a personal identification number (PIN) familiar from many other contexts.

EX1009, 3:7-12 (emphasis added). See also *id.*, 7:36-8:2 (the user “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.”) (emphasis added).

Further, the “identity code” and the “user identification code” are not the same thing. *Kew*’s system “uses the user identification code (USER ID) to access its database to locate the corresponding identity code for the appropriate receiver unit.”). *Id.*, 11:8-11 (emphasis added). See also *id.*, 7:34-8:5 (“When the user seeks access to the host system 1 via the terminal 2, he enters his user identification code

. . . The security server 5 includes a database of all authorised users and their authorised receiver units 6, and identifies the corresponding identity code for the appropriate receiver unit 6.”) (emphasis added). Accordingly, *Kew*’s “user identification code” is used to lookup, within a database, the appropriate “identity code.” If *Kew*’s “user identification code” and “identity code” were the same, the “identity code” would be known as soon as the “user identification code” was known, and there would be no need to look it up. Accordingly, *Kew*’s “user identification code” and *Kew*’s “identity code” are not the same.

Second, *Kew* also fails to disclose the claimed “token.” Claim element 5[c] requires that “the token is not known to the user.” EX1001, 12:29-30. Based on the specification, a POSITA would interpret “not known to the user” to mean “not known to the user before being sent to the user as part of the authentication process.” *See id.*, 4:52-53 (“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.

Petitioner concedes that is the correct interpretation because under Ground 1, the Petition mapped *Veneklase*’s “random code” to the claimed “token.” *See* Pet, p. 24 (“*Veneklase* teaches . . . a token that is not known to the user beforehand (e.g., random code)”). And it is undisputed that *Veneklase*’s “random code” is eventually

known to the user. *See* EX1005, 8:18-19 (“user 404 now enters the code he or she has received from the pager”).

Further, that is also how the Unified IPR interpreted “not known to the user.” *See* IPR2023-00425, Paper 1 at 10-13 (P.T.A.B. Jan. 6, 2023) (“[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.”) (emphasis added). And the instant Petition “substantially adopts the unpatentability grounds and arguments raised in [the Unified IPR].” Pet., p. 1. But the Petition provides zero evidence that *Kew*’s “Code A” is eventually known to the user. *See id.* at 62-64. 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* EX1009, 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 the proper interpretation (and Petitioner’s interpretation) of claim element 5[c] requires. 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.

In view of the above, *Kew* fails to teach or suggest claim element 5[c]. *Sormunen* does not cure the deficiencies of *Kew*, and the Petition does not so allege. *See* Pet., pp. 62-64. Accordingly, the combination of *Kew* and *Sormunen* does not teach or suggest this claim element.

- ii. 5[f] “wherein the authentication module . . . deactivates the account within a predetermined amount of time after activating the account”

As discussed above with respect to Ground 1, claim element 5[f] requires that an “authentication module” activate access to the account in response to the creation of the password, which starts a “predetermined amount of time,” and that the “authentication module” deactivate the account upon expiration of the “predetermined amount of time.” EX1001, 12:41-45.

Kew discloses that “the receiver can only be enabled for a predetermined period to permit it to transform the received Code A to the transformed Code C by input of a second user identification code by the user.” EX1009, 3:14-17 (emphasis added). The “predetermined period” is merely how long *Kew*’s “receiver unit” remains activated once it has been activated via user input of the “second user identification code.” *Id.* As disclosed by *Kew*, it would be a security risk to have the “receiver unit” permanently activated in case an unauthorized user acquires possession of it. *See* EX1009, 3:14-23.

In one instance, Petitioner mapped the “predetermined period” that *Kew’s* “receiver unit” remains activated (once the user enters the “second user identification code”) to the claimed “predetermined amount of time.” Pet., p. 69. That mapping is flawed. Even if *Kew’s* “security server” (Petitioner-identified “authentication module”) knows the “predetermined period” is *X* minutes, neither Petitioner nor its expert explain how *Kew’s* “security server” knows when the *X* minutes start or ends. See Pet., p. 69; EX1002, ¶178. Thus, *Kew’s* “security server” (Petitioner-identified “authentication module”) has no way of knowing when to deactivate the account, as claim 5 requires. Further, *Kew’s* “predetermined period” starts when *Kew’s* “receiver unit” is activated by the user. In contrast, the claimed “predetermined amount of time” starts with the “authentication module” activating access to the account.

In one instance, Petitioner mapped the “predetermined length of time” that *Kew’s* “receiver unit” displays “Code C” to the claimed “predetermined amount of time.” Pet., p. 69. That mapping is also flawed. Again, even if *Kew’s* “security server” (Petitioner-identified “authentication module”) knows the “predetermined length” is *Y* minutes, neither Petitioner nor its expert explains how *Kew’s* “security server” knows when the *Y* minutes start or end. See Pet., p. 69; EX1002, ¶179. Thus, *Kew’s* “security server” (Petitioner-identified “authentication module”) has no way

of knowing when to deactivate the account, as claim 5 requires. Further, *Kew*'s "predetermined length of time" starts when *Kew*'s "receiver unit" starts displaying "Code C." In contrast, the claimed "predetermined amount of time" starts with the "authentication module" activating access to the account.

In view of the above, *Kew* fails to teach or suggest claim element 5[f]. *Sormunen* does not cure the deficiencies of *Kew*, and the Petition does not so allege. See Pet., pp. 67-70. Accordingly, the combination of *Kew* and *Sormunen* does not render independent claim 5 obvious.

2. Dependent Claim 7

Petitioner mapped *Kew*'s "receiver unit 6" and "Code A" to the claimed "personal communication device" and claimed "token," respectively. See Pet., pp. 60, 64. *Kew* alone, however, does not disclose claim 7 because *Kew* expressly discloses that the request comes from "terminal 2," which is a different device than the "personal communication device" identified by Petitioner (i.e., "receiver unit 6"). See Pet., p. 60; see also EX1009, 7:34-8:10. Petitioner's proposed combination of *Kew* and *Sormunen* fails to support a conclusion of obviousness for multiple reasons.

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* EX1009, 2:25-36, 7:34-9:11. Those are the fundamental steps of *Kew*’s authentication process, and thus those steps define *Kew*’s principle of operation.

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. 71-72 (citing EX1007, 5:38-61, Fig. 2). But that modification changes the fundamental steps in *Kew*’s authentication process, and thus changes *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 7 obvious. *See* MPEP § 2143.01(VI) (citing *In re Ratti*, 270 F.2d 810, 813 (CCPA 1959)).

Additionally, or alternatively, the system in *Kew* transmits “Code A” (Petitioner-identified “token”) in response to receiving *Kew*’s “user identification code.” EX1009, 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”). But *Kew* also requires that the “user identification code” be transmitted to *Kew*’s system via *Kew*’s “terminal.” See EX1009, 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.” EX1009, 7:10-18, 9:5-7, Fig. 1 (showing multiple terminals). Accordingly, Petitioner’s proposed combination requires transmitting *Kew*’s “user identification code” twice, from two separate devices, for a single session with *Kew*’s system.

Kew discloses the “user identification code” is “preferably a more secure code such as a PIN.” EX1009, 8:1-2. Increasing the number of times the “user identification code” is transmitted only increased the likelihood of it being intercepted. Accordingly, that double transmission of *Kew*’s “user identification code” with no ascertainable benefit is not rational. Thus, Petitioner’s proposed modification does not render claim 7 obvious. See *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007).

Petitioner argues a POSITA would have modified *Kew* based on *Sormunen* because “*Kew*’s system would obtain *Sormunen*’s benefits of allowing for secure

access to a service ‘almost immediately’ after a request is sent. EX1007, 5:12-18 (the ‘present invention enables very fast subscription,’ and ‘[a] further advantage of the fast data transmission is that...security may thus be improved’).” *See* Pet., pp. 73-76; EX1002, ¶¶192-193. But neither Petitioner nor its expert offer any evidence that *Kew*’s modified system would be faster or more secure than *Kew*’s original system. *See id.* *Sormunen*’s use of “very fast” and “almost immediately” is a comparison with older systems that utilize the postal service or that require a human review for a subscription request. *See* EX1007, 3:6-4:16. But *Kew* is not one of those older systems.

Further, the alleged security in *Sormunen* arises from transmission of sensitive data from the system to the user’s cellphone/pager. *See* EX1007, 4:18-24 (“An object of the present invention is to eliminate the disadvantages disclosed above and to establish a method wherein transmission of user specific authentication data from the service provider to the user of the service can be performed as fast and as safely as possible. The invention is based on the idea that user specific authentication data is transmitted to the user by using, at least partly, a paging system or a short message service.”) (emphasis added). Again, *Kew*’s original system already transmits sensitive data (i.e., code A) to the user’s pager. *See* EX1009, 1:31 (“transmitting Code A via a paging system”), 8:12-14 (“the security server 5 also transmits the

random [Code A] to a paging system 7”). Accordingly, there is no motivation to modify *Kew* based on *Sormunen*.

Petitioner argues the *Kew-Sormunen* combination “would offer increased security by ensuring that tokens are only sent to devices already in the hands of the user at the time of the request, rather than to a device that may have been misplaced or even lost.” Pet., pp. 75-76. Petitioner is misguided. If the user has misplaced or lost their device (e.g., pager/cellphone), the user would not even attempt to use the *Kew* system knowing that “Code A” (Petitioner-identified “token”) would be sent to the misplaced/lost device. Accordingly, the alleged “increased security” resulting from the combination with *Sormunen* is non-existent.

For these reasons, the combination of *Kew* and *Sormunen* does not render claim 7 obvious.

H. Ground 4 – The Combination of *Kew*, *Sormunen*, and *Kaufman* Does Not Render Obvious Dependent Claim 2.

Claim 2 depends from claim 1. Accordingly, claim 2 has all the requirements of claim 1. 35 U.S.C. § 112, ¶4. The Petition’s defects regarding claim 1 are discussed before the defects specific to claim 2.

1. Independent Claim 1

As a threshold matter, Petitioner does not rely on *Kaufman* to teach or suggest any element of claim 1. See Pet., pp. 77-78. Further, Petitioner argues “claim 1

recites limitations analogous in scope to those of claim 5.” *Id.* As discussed above, the combination of *Kew* and *Sormunen* fails to teach or suggest claim elements 5[c] and 5[f]. Accordingly, the combination also fails to teach or suggest the corresponding claim elements in independent claim 1. Petitioner argues that claim element 1[b] is analogous to claim 7. *See id.* As discussed above, the combination of *Kew* and *Sormunen* fails to render obvious claim 7, and thus also fails to render obvious claim element 1[b].

2. Dependent Claim 2

As a threshold matter, the combination of *Kew* and *Sormunen* fails to render claim 1 unpatentable (discussed above). *Kaufman* does not cure the deficiencies of *Kew* and *Sormunen*, and the Petition does not assert otherwise. *See Pet.*, pp. 77-83. Accordingly, the combination of *Kew*, *Sormunen*, and *Kaufman* fails to render claim 1 unpatentable. Claim 2 depends from and adds limitations to claim 1. Thus, the combination of *Kew*, *Sormunen*, and *Kaufman* fails to render claim 2 unpatentable for at least the same reasons.

Further, as discussed under Ground 2 (above), *Kaufman* with its necessary “authentication token generator,” teaches away from the claimed invention and cannot render the claimed invention obvious.

Further still, Petitioner argued that *Kew* “does not disclose details of what particular algorithm is utilized” and thus a “POSITA reviewing *Kew* and looking to implement its system would be motivated to look to another reference, like *Kaufman*, that provides further details about exemplary one-way algorithms.” Pet., p. 82 (emphasis added). That is misleading and simply untrue. *Kew* discloses it is using a one-way encryption algorithm with the “identity code” as an encryption key to encrypt “Code A.” See EX1009, 7:29-32 (*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.”) (emphasis added). In contrast, *Kaufman* criticizes the use of encryption algorithms/keys, and thus teaches away from their use. See EX1008, 3:9-5:8. Petitioner even concedes that is the case. See Pet., p. 54 (“*Kaufman* includes a detailed discussion of prior encryption techniques and parts of the downfalls of these different systems.”) (emphasis added). Accordingly, a POSITA would not be looking to *Kaufman* for the implementation details pertaining to *Kew*’s encryption algorithm/key.

There is no motivation to combine *Kaufman* with *Kew* and *Sormunen*.

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(d), I hereby certify that the foregoing Patent Owner Response contains 13,916 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: April 22, 2024

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 April 22, 2024, 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 (Alexander B. Stein, Ahren C. Hsu-Hoffman, Austin L. Zuck) at the following address:

MLB_Dynapass-Amazon@morganlewis.com

Respectfully submitted,

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