

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

AMAZON.COM, INC.,

Petitioner,

v.

DYNAPASS IP HOLDINGS LLC,

Patent Owner.

Case No. IPR2024-00283

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

**PETITION FOR *INTER PARTES* REVIEW OF
CLAIMS 2 and 7 OF U.S. PATENT NO. 6,993,658**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. MANDATORY NOTICES	1
A. Real Party-in-Interest (37 C.F.R. § 42.8(b)(1)).....	1
B. Related Matters (37 C.F.R. § 42.8(b)(2)).....	2
C. Counsel (37 C.F.R. § 42.8(b)(3)) and Service Information (37 C.F.R. § 42.8(b)(4)).....	4
III. CERTIFICATION AND FEES	5
IV. IDENTIFICATION OF CLAIMS AND GROUNDS.....	5
V. DISCRETIONARY DENIAL WOULD BE INAPPROPRIATE.....	6
A. §325(d) – The Board Should Not Deny Institution.....	6
B. § 314(a) – <i>Fintiv</i> Does Not Support Denial	7
C. <i>General Plastic</i> Does Not Support Denial	7
VI. BACKGROUND	11
A. The '658 Patent	11
B. Cited References.....	12
1. Kaufman (Ex.1008).....	13
2. Sormunen (Ex.1007)	14
VII. LEVEL OF ORDINARY SKILL	14
VIII. CLAIM CONSTRUCTION	15
IX. GROUND #1: CLAIM 7 IS OBVIOUS OVER <i>VENEKLASE</i> IN VIEW OF <i>JONSSON</i> AND <i>SORMUNEN</i>	16
A. Claim 5	16
1. 5[pre]—“A user authentication system comprising:”.....	16
2. 5[a]—“a computer processor;”	17

TABLE OF CONTENTS
(continued)

	Page
3. 5[b]—“a user database configured to associate a user with a personal communication device possessed by the user, said personal communication device configured to communicate over a cell phone network with the user authentication system;”	18
4. 5[c]—“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;”	22
5. 5[d]—“a communication module configured to transmit the token to the personal communication device through the cell phone network; and”	26
6. 5[e]—“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,”	28
7. 5[f]—“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 a secure computer network.”	31
B. Ample Motivation Existed to Combine <i>Veneklase</i> and <i>Jonsson</i>	35
C. Claim 6	39
D. Claim 7	41
E. Ample Motivation Existed to Combine <i>Veneklase</i> , <i>Jonsson</i> , and <i>Sormunen</i>	44

TABLE OF CONTENTS
(continued)

	Page
X. GROUND #2: CLAIM 2 IS OBVIOUS OVER <i>VENEKLASE</i> IN VIEW OF <i>JONSSON</i> , <i>SORMUNEN</i> , AND <i>KAUFMAN</i>	47
A. Claim 1	48
1. 1[b]—“receiving a request from the user for a token via the personal communication device, over the second network;”	48
B. Claim 2	50
C. Ample Motivation Existed to Combine <i>Veneklase</i> , <i>Jonsson</i> , <i>Sormunen</i> , and <i>Kaufman</i>	52
XI. GROUND #3: CLAIM 7 IS OBVIOUS OVER <i>KEW</i> IN VIEW OF <i>SORMUNEN</i>	55
A. Claim 5	55
1. 5[pre]	55
2. 5[a]	56
3. 5[b]	57
4. 5[c]	62
5. 5[d]	64
6. 5[e]	65
7. 5[f].....	67
B. Claim 6	70
C. Claim 7	71
D. Ample Motivation Existed to Combine <i>Kew</i> and <i>Sormunen</i>	73
XII. GROUND #4: CLAIM 2 IS OBVIOUS OVER <i>KEW</i> IN VIEW OF <i>SORMUNEN</i> AND <i>KAUFMAN</i>	77
A. Claim 1	77

TABLE OF CONTENTS
(continued)

	Page
1. 1[b]—“receiving a request from the user for a token via the personal communication device, over the second network;”	78
B. Claim 2	78
C. Ample Motivation Existed to Combine <i>Kew</i> , <i>Sormunen</i> , and <i>Kaufman</i>	80
XIII. NO SECONDARY CONSIDERATIONS SUPPORT NON-OBVIOUSNESS	83
XIV. CONCLUSION.....	83

PETITIONER’S EXHIBIT LIST

Exhibit	Description
1001	U.S. Patent No. 6,993,658 to Engberg et al. (the “’658 Patent”)
1002	Declaration of Expert Dr. Jon Weissman
1003	<i>Curriculum Vitae</i> of Expert Dr. Jon Weissman
1004	File History of the ’658 Patent
1005	European Patent Application No. 0844551 to Veneklasé (“Veneklasé”)
1006	PCT Patent Publication No. WO 96/00485 to Jonsson (“Jonsson”)
1007	PCT Patent Publication No. WO 97/31306 to Sormunen (“Sormunen”)
1008	U.S. Patent No. 5,491,752 to Kaufman et al. (“Kaufman”)
1009	PCT Patent Publication No. WO 95/19593 to Kew (“Kew”)
1010	Amazon.com <i>Sotera</i> Stipulation
1011	Claim Construction Order, <i>Dynapass IP Holdings LLC v. JPMorgan Chase & Co.</i> , No. 2:22-cv-00212-JRG-RSP (E.D. Tex. Oct. 31, 2023).
1012	Petition for <i>Inter Partes</i> Review in <i>Unified Patents, LLC v. Dynapass IP Holdings LLC</i> , IPR2023-00425, Paper 1 (PTAB Jan. 6, 2023)
1013	Unified Patents Institution Decision, IPR2023-00425, Paper 9 (July 18, 2023)

I. INTRODUCTION

Amazon.com, Inc. (“Petitioner”) requests *Inter Partes* Review (“IPR”) of dependent claims 2 and 7 (the “Challenged Claims”) of U.S. Patent No. 6,993,658 (the “’658 Patent”), purportedly assigned to Dynapass IP Holdings LLC (“PO”). This Petition presents a streamlined approach to reviewing claims 2 and 7 because it substantially adopts the unpatentability grounds and arguments raised in another IPR proceeding challenging claims 1 and 5-6, but not challenging claims 2 and 7. *See Unified Patents, LLC v. Dynapass IP Holdings LLC*, IPR2023-00425 (PTAB Jan. 6, 2023) (“Unified IPR”) (instituted July 18, 2023). By adopting substantially the same unpatentability grounds and arguments, the Board’s analysis of independent claims 1 and 5 in conjunction with the Unified IPR will apply here as well, thus eliminating the need for the Board to re-analyze those independent claims. Here, the Board need only resolve whether the few additional limitations of claims 2 and 7 save them from cancellation. This Petition demonstrates—using a streamlined approach that furthers “efficient administration of the Office” (35 U.S.C. § 311(b))—that those few additional limitations add nothing. Claims 2 and 7 should be cancelled.

II. MANDATORY NOTICES

A. Real Party-in-Interest (37 C.F.R. § 42.8(b)(1))

The real party-in-interest is Petitioner.

B. Related Matters (37 C.F.R. § 42.8(b)(2))

The '658 Patent is presently the subject of a patent infringement lawsuit brought by PO against Petitioner captioned *Dynapass IP Holdings LLC v. Amazon.com, Inc.*, Case No. 2:23-cv-00063-JRG-RSP (E.D. Tex.) (the “Related Litigation”).

Petitioner is aware of the following district court proceedings involving the '658 Patent:

- *Dynapass IP Holdings LLC v. Woodforest National Bank et al.*, 2:22-cv-00218 (E.D. Tex. filed June 17, 2022);
- *Dynapass IP Holdings LLC v. Wells Fargo & Company et al.*, 2:22-cv-00217 (E.D. Tex. filed June 17, 2022);
- *Dynapass IP Holdings LLC v. PNC Financial Services et al.*, 2:22-cv-00214 (E.D. Tex. filed June 17, 2022);
- *Dynapass IP Holdings LLC v. JPMorgan Chase & Co. et al.*, 2:22-cv-00212 (E.D. Tex. filed June 17, 2022) (“JPMorgan Case”);
- *Dynapass IP Holdings LLC v. BOKF, National Association et al.*, 2:22-cv-00211 (E.D. Tex. filed June 17, 2022);
- *Dynapass IP Holdings LLC v. Truist Financial Corporation et al.*, 2:22-cv-00216 (E.D. Tex. filed June 17, 2022);

- *Dynapass IP Holdings LLC v. Regions Financial Corporation et al.*, 2:22-cv-00215 (E.D. Tex. filed June 17, 2022);
- *Dynapass IP Holdings LLC v. PlainsCapital Bank et al.*, 2:22-cv-00213 (E.D. Tex. filed June 17, 2022);
- *Dynapass IP Holdings LLC v. Bank of America Corporation et al.*, 2:22-cv-00210 (E.D. Tex. filed June 17, 2022);
- *Dynapass Inc. v. Mobile Authentication Corporation et al.*, 8:18-cv-01173 (C.D. Cal. July 3, 2018);
- *Dynapass IP Holdings LLC v. Simmons First National Corporation et al.*, 2:23-cv-00068 (E.D. Tex. filed February 20, 2023);
- *Dynapass IP Holdings LLC v. First Citizens Bancshares, Inc. et al.*, 2:23-cv-00067 (E.D. Tex. filed February 20, 2023);
- *Dynapass IP Holdings LLC v. Experian Information Services, Inc.*, 2:23-cv-00066 (E.D. Tex. filed February 20, 2023);
- *Dynapass IP Holdings LLC v. East West Bancorp, Inc. et al.*, 2:23-cv-00065 (E.D. Tex. filed February 20, 2023);
- *Dynapass IP Holdings LLC v. The Charles Schwab Corporation et al.*, 2:23-cv-00064 (E.D. Tex. filed February 20, 2023);

- *Jack Henry & Associates, Inc. v. Dynapass IP Holdings LLC*, 1:23-cv-00388 (D. Del. filed April 5, 2023);

In addition to the Unified IPR, Petitioner is also aware that the '658 Patent has been challenged at the PTAB in the following IPRs (the "Related IPRs"):

- *Bank of America, NA et al. v. Dynapass IP Holdings LLC*, IPR2023-00367 (PTAB Jan. 3, 2023) ("BofA IPR");
- *JPMorgan Chase Bank, NA v. Dynapass IP Holdings LLC*, IPR2023-01331 (PTAB Aug. 16, 2023) ("Chase IPR");
- *Experian Information Solutions, Inc. v. Dynapass IP Holdings LLC*, IPR2023-01406 (PTAB Sept. 28, 2023) ("Experian IPR").

The Unified IPR was instituted by the PTAB on July 18, 2023. The Chase IPR seeks to join the instituted Unified IPR proceedings.

C. Counsel (37 C.F.R. § 42.8(b)(3)) and Service Information (37 C.F.R. § 42.8(b)(4))

Petitioner designates Alexander B. Stein (Reg. No. 71,397) as lead counsel, and Ahren C. Hsu-Hoffman (Reg. No. 50,862) and Austin L. Zuck (Reg. No. 81,341) as back-up counsel.

Postal and hand deliveries for lead and back-up counsel should be addressed to: Morgan, Lewis & Bockius LLP, 1400 Page Mill Road, Palo Alto, CA 94304 (Telephone: 650.843.4000; Fax: 650.843.4001).

Pursuant to 37 C.F.R. §42.8(b)(4), Petitioner consents to e-mail service at:
MLB_Dynapass-Amazon@morganlewis.com.

Pursuant to 37 C.F.R. § 42.10(b), a Power of Attorney is filed concurrently
herewith.

III. CERTIFICATION AND FEES

Petitioner certifies that the '658 Patent is available for IPR and that
Petitioner is not barred/estopped from requesting this IPR.

The required fees are submitted herewith in accordance with 37 C.F.R. §§
42.103(a), 42.15(a). Any additional fees may be charged to Deposit Account No.
50,0310 (Order No. 049673-2616).

IV. IDENTIFICATION OF CLAIMS AND GROUNDS

The '658 Patent issued from U.S. Patent Application No. 09/519,829, filed
March 6, 2000, which for purposes of this proceeding only, Petitioner treats as the
Priority Date.

Petitioner relies on the following prior art references, none of which were
considered by the Patent Office during prosecution:

Veneklase (Ex.1005): European Patent Application No. 0844551 (published
May 27, 1998) is prior art under § 102(b).¹

¹ Citations to §§ 102 and 103 are to the pre-AIA statutes.

Jonsson (Ex.1006): PCT Patent Publication No. WO96/00485 (published January 4, 1996) is prior art under § 102(b).

Sormunen (Ex.1007): PCT Patent Publication No. WO97/31306 (published August 28, 1997) is prior art under § 102(b).

Kaufman (Ex.1008): U.S. Patent No. 5,491,752 (issued February 13, 1996) is prior art under § 102(b).

Kew (Ex.1009): PCT Patent Publication No. WO95/19593 (published July 20, 1995) is prior art under § 102(b).

Petitioner challenges claims 2 and 7 using 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

V. DISCRETIONARY DENIAL WOULD BE INAPPROPRIATE

A. §325(d) – The Board Should Not Deny Institution

The Office’s resources would be well used in considering claims 2 and 7, particularly given this Petition’s streamlined approach. While this Petition does rely on four references presented in the Unified IPR to provide the Board with a streamlined way to review claims 2 and 7 (which are not challenged in the Unified

IPR), § 325(d) is still no bar to institution. For example, *Sormunen* is used in combination with *Veneklase* and *Jonsson* here, which is an obviousness combination not presented in the Unified IPR. Further, *Kaufman* is a new reference that has not been considered by the Office (either in the IPRs² or during prosecution).

B. § 314(a) – *Fintiv* Does Not Support Denial

“[T]he PTAB will not discretionarily deny institution in view of parallel district court litigation where a petitioner presents a stipulation not to pursue in a parallel proceeding the same grounds or any grounds that could have reasonably been raised.” Director Vidal’s Memorandum issued June 21, 2022. Here, Petitioner has stipulated that it will not pursue the same grounds that (1) are or could have reasonably been raised in this Petition, and (2) are or could have reasonably been raised in the Unified IPR.

C. *General Plastic* Does Not Support Denial

While this Petition does follow other petitions temporally, it does not present the types of issues identified by the Board in *General Plastics*.

² The BofA IPR cited to *Kaufman* for background, but it was not asserted in any ground of unpatentability.

GP Factor 1. Petitioner has not previously filed a petition directed to the '658 Patent. Further, Petitioner has had no “significant relationship” with any of the petitioners in the Related IPRs like the one described in *Valve v. Electronic Scripting*, IPR2019-00062, Paper 11, 10 (PTAB Apr. 2, 2019) (precedential); *see Mercedes-Benz v. Carucel*, IPR2019-01404, Paper 12, 12 (PTAB Jan. 22, 2020) (finding even membership in Unified Patents did not justify discretionary denial); *Netflix Inc. & Hulu, LLC v. DIVX, LLC*, IPR2020-00052, Paper 42, 10-11 (May 14, 2020) (same).

This factor weighs heavily against denial.

GP Factor 2. Petitioner first learned of the '658 Patent from the complaint against Petitioner filed on February 20, 2023. Petitioner was thus not previously aware of the unpatentability of this patent—including the prior art raised in the BofA and Unified IPRs.

This factor weighs heavily against denial.

GP Factor 3. Although this Petition is filed after the PO Preliminary Responses were filed and the Institution Decisions were rendered in the BofA and Unified IPRs, and the PO Response was filed in the Unified IPR, Petitioner is not using this Petition to address any deficiencies that have been alleged concerning the grounds raised in those proceedings. *See Code200, UAB v. Bright Data Ltd.*, IPR2022-00861, Paper 18 at 5 (PTAB Aug. 23, 2022) (precedential) (“[R]oad-

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.”).

Rather, Petitioner is challenging two dependent claims, claims 2 and 7, not challenged in the Unified IPR, by adopting the unpatentability positions presented by Unified³ as to the claims from which claims 2 and 7 depend (*i.e.*, claims 1 and 5-6) and supplementing those positions to specifically address claims 2 and 7, which the Unified IPR did not challenge. The Office has also not previously been presented with the question of whether a combination involving *Kaufman* renders claim 2 obvious. Also, this Petition is being filed before any PO Preliminary Response in the Experian IPR.

This factor weighs against denial, or is (at worst) neutral.

GP Factors 4-5. As previously discussed under Factor 2, Petitioner was unaware of the asserted prior art in the BofA and Unified IPRs, as the petitions for these IPRs were filed nearly two months before the complaint was filed against Petitioner. This Petition is filed just a few months after the institution decisions in those IPRs to address two dependent claims that will not be addressed in the

³ Petitioner’s grounds are different from those raised in the BofA IPR.

instituted Unified IPR proceeding, and just a few months after Petitioner served PO with its invalidity contentions.

This factor weighs against denial.

GP Factor 6. Efficiency considerations strongly favor institution. This Petition adopts the same grounds as the Unified IPR for claims 1 and 5-6 and merely supplements them to address the peripheral limitations of dependent claims 2 and 7, which together amount to a mere five (5) lines of text and recite nothing novel. As such, it will be exceedingly efficient for the Board to address the validity of these two minor dependent claims. *See Code200*, Paper 18 at 6 (“[T]he Board’s mission ‘to improve patent quality and restore confidence in the presumption of validity that comes with issued patents’ outweighs the impact on Board resources needed to evaluate the merits of a petition.”).

This factor weighs heavily against denial.

GP Factor 7. Nothing precludes the Board from issuing a Final Written Decision within a year of institution.

This factor weighs heavily against denial.

VI. BACKGROUND

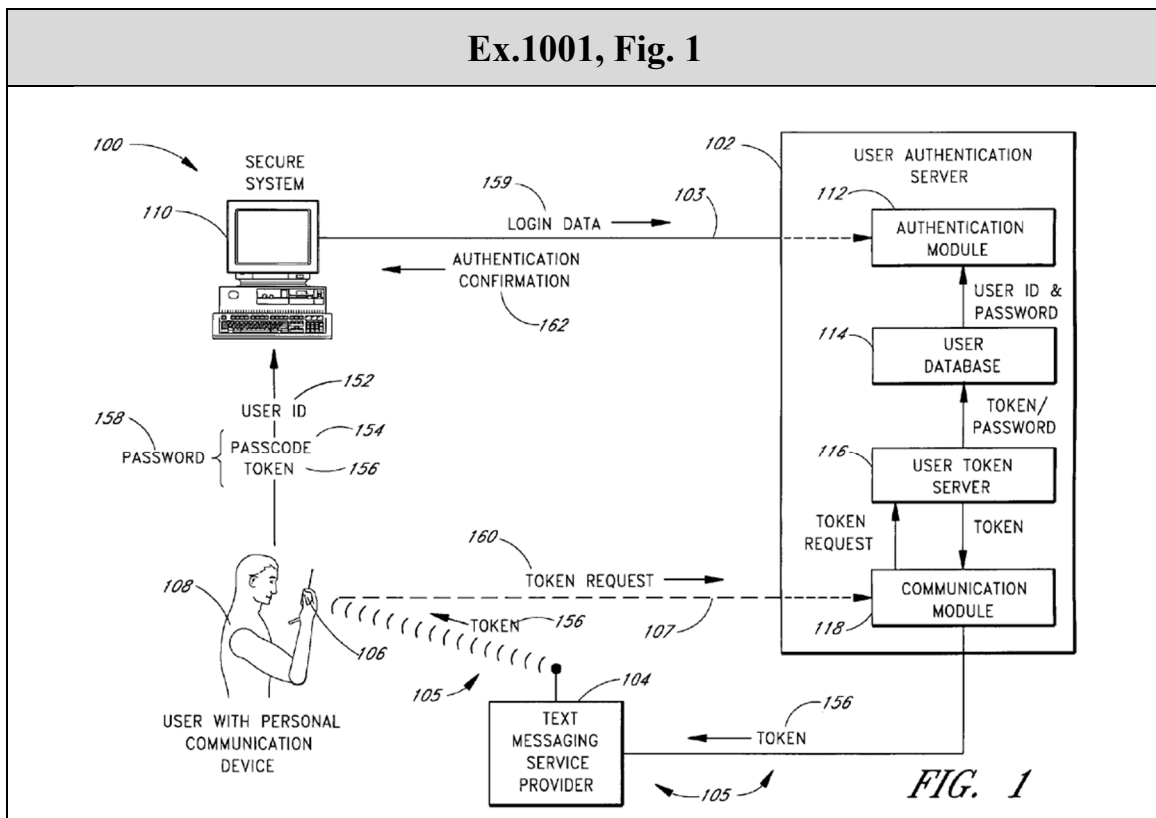
A. The '658 Patent

The '658 Patent concerns two-factor authentication. Two-factor authentication uses two factors (*e.g.*, known password and randomly generated code) to verify a user's identity when logging into a secure system.

The '658 Patent acknowledges that the named inventors did not invent two-factor authentication. *See* Ex.1001, 1:44-53 (admitting that “[t]he SecurID product” already “require[ed] a two-factor authentication process”).

The '658 Patent purports to replace the SecureID card by using “a personal communication device such as a mobile phone or a pager” to obtain the benefits of the SecurID product in “a device that many users already carry.” *Id.*, at 1:57-59. As shown in Figure 1, in response to a user's token request 160, user token server 116 generates a token 156 (*e.g.*, randomly generated code) and creates a new password 158 based on the user's passcode 154 (*e.g.*, secret password known to user) and the token 156. Ex.1001, 6:59-63, 2:11-15.⁴ The token 156 is transmitted to the user's personal communication device 106 so the user can use it to log in. *Id.*, 7:31-63, 9:60-64; *see* Ex.1012, 7-9.

⁴ Emphasis in textual quotations and annotations/coloring in figures are added throughout, unless otherwise noted.



Challenged claim 2 merely requires that “the new password is generated by concatenating the token and the passcode.” Challenged claim 7 merely requires that “the request is transmitted by the user through the personal communication device,” which is similarly required by limitation 1[b]. Ex.1002, ¶¶46-50.

B. Cited References

Summaries of the *Veneklase*, *Jonsson*, *Sormunen*, *Kaufman*, and *Kew* references have been provided in conjunction with the Unified IPR. Ex.1012, 18-22, 51-55; Ex.1002, ¶¶52-63. *Kaufman* was not previously considered, and a short summary—focusing on its relevance to claim 2’s trivial “concatenating” limitation—is provided. *Sormunen*, while raised in the previous IPRs, was not

relied on in combination with *Veneklase* and *Jonsson*, and thus a refresher on *Sormunen* (particularly as to claim 7) is provided below.

1. Kaufman (Ex.1008)

Kaufman discloses “a workstation [that] exchanges data with an authentication server to obtain access to a desired computing system.” Ex.1008, 6:50-52. “[T]he user initiates communications with the authentication server by entering his ‘password’ into the workstation” and “enters a token provided by the passive token generator.” *Id.*, 6:66-7:2. The workstation “calculates a ‘transmission code’ by applying a first, cryptographically secure hashing algorithm to the password and the token, so that this information can be securely sent to the server.” *Id.*, 7:2-5.

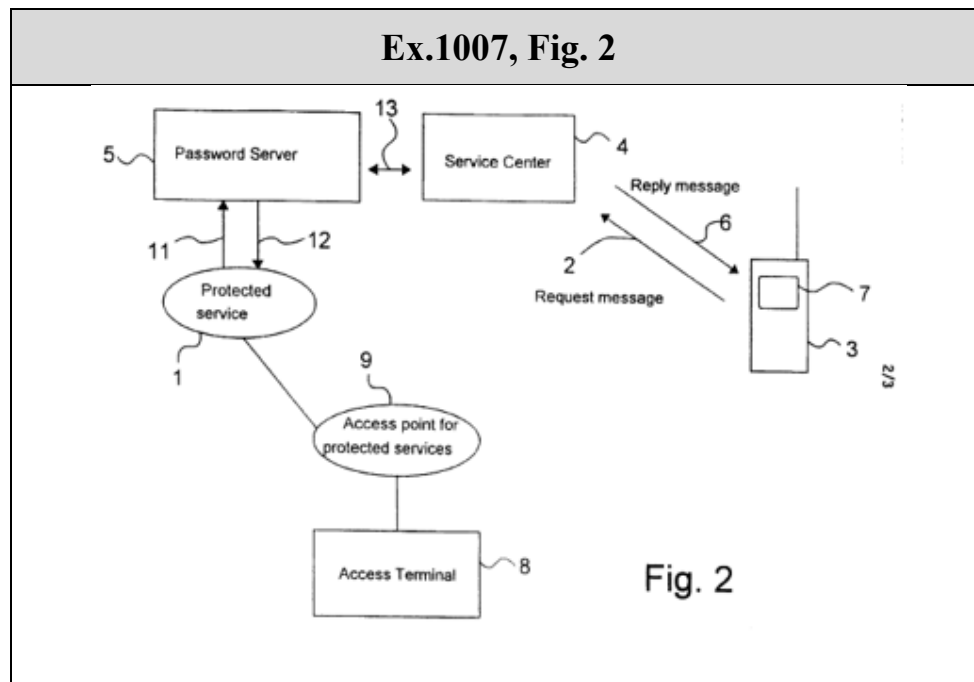
Kaufman’s “hashing algorithms” show “a one-way routine for transmuting multiple input data items, by **concatenating** selected items of the input data.” *Id.*, 9:43-47; Ex.1002, ¶¶58-60.

Ex.1008, 9:65-10:5 – Hashing Algorithms Disclosed in <i>Kaufman</i>	
[1.0]	hash(token hash(password))
[1.1]	hash(hash(password) token)
[1.2]	hash(token password)
[1.3]	hash(password token)

Therefore, *Kaufman* discloses the “concatenating” requirements of claim 2.

2. Sormunen (Ex.1007)

Sormunen teaches (1) sending a “password request” from the user via a mobile phone (first device) to a password server (second device), (2) transmitting the password to the mobile phone over a mobile communication network, and (3) submitting the password to the password server via an access terminal (third device) for authentication. *Id.*, 5:33-7:18, Fig. 2; Ex.1002, ¶¶56-57.



Therefore, *Sormunen* discloses claim 7’s requirement of a token “request [] transmitted by the user through the personal communication device.”

VII. LEVEL OF ORDINARY SKILL

A POSITA would have had at least (1) an undergraduate degree in electrical and computer engineering or a closely related field; and (2) two or more years of experience in security. Additional advanced education could substitute for some

years of experience, and, likewise, additional industry experience could substitute for education. Ex.1002, ¶¶15-19.

VIII. CLAIM CONSTRUCTION

Magistrate Judge Payne in the JPMorgan Case recently construed the following terms:

Term	Court's Construction
“concatenating”	“joining sequentially”
“receiving a request from the user for a token via the personal communication device, over the second network”	“receiving, over the second network via the personal communication device, a request from the user for a token”
“activates access to the account in response to the password”	“activates access to the account in response to the creation of the password”
“activating access the user account on the first secure computer network”	Plain and ordinary meaning
“password”	Plain and ordinary meaning

Ex.1011, 16.

Judge Payne’s construction of the “activates access...” limitation was based on Dynapass’s disclaimer in the BofA and Unified IPRs (*id.*, 10-13), which was found to apply only to claim 5. Judge Payne found that there was no disclaimer for the “activating access...” limitation in claim 1 and afforded that phrase its plain-and-ordinary meaning.

Petitioner submits the claims are obvious under Judge Payne’s or any reasonable construction of the above terms, and that all other terms should be

given their plain meaning. Ex.1002, ¶¶41-45.

IX. GROUND #1: CLAIM 7 IS OBVIOUS OVER *VENEKLASE* IN VIEW OF *JONSSON* AND *SORMUNEN*

Independent claim 5 of the '658 Patent will be considered first. Claim 7 depends from claim 6, which depends from claim 5. *Veneklase*, in view of *Jonsson* and *Sormunen*, renders the limitations of claims 5 and 6 obvious, as discussed below. Claim 7 adds that the “request is transmitted by the user through the personal communication device.”⁵

Petitioner adopts Unified’s positions as to the combination of *Veneklase* and *Jonsson* for claim 5 and for *Sormunen*’s teaching concerning claim 1[b]’s recitation of “receiving a request from the user for a token via the personal communication device....” Petitioner applies *Sormunen*’s teaching to show the similar limitation present in claim 7 is obvious.

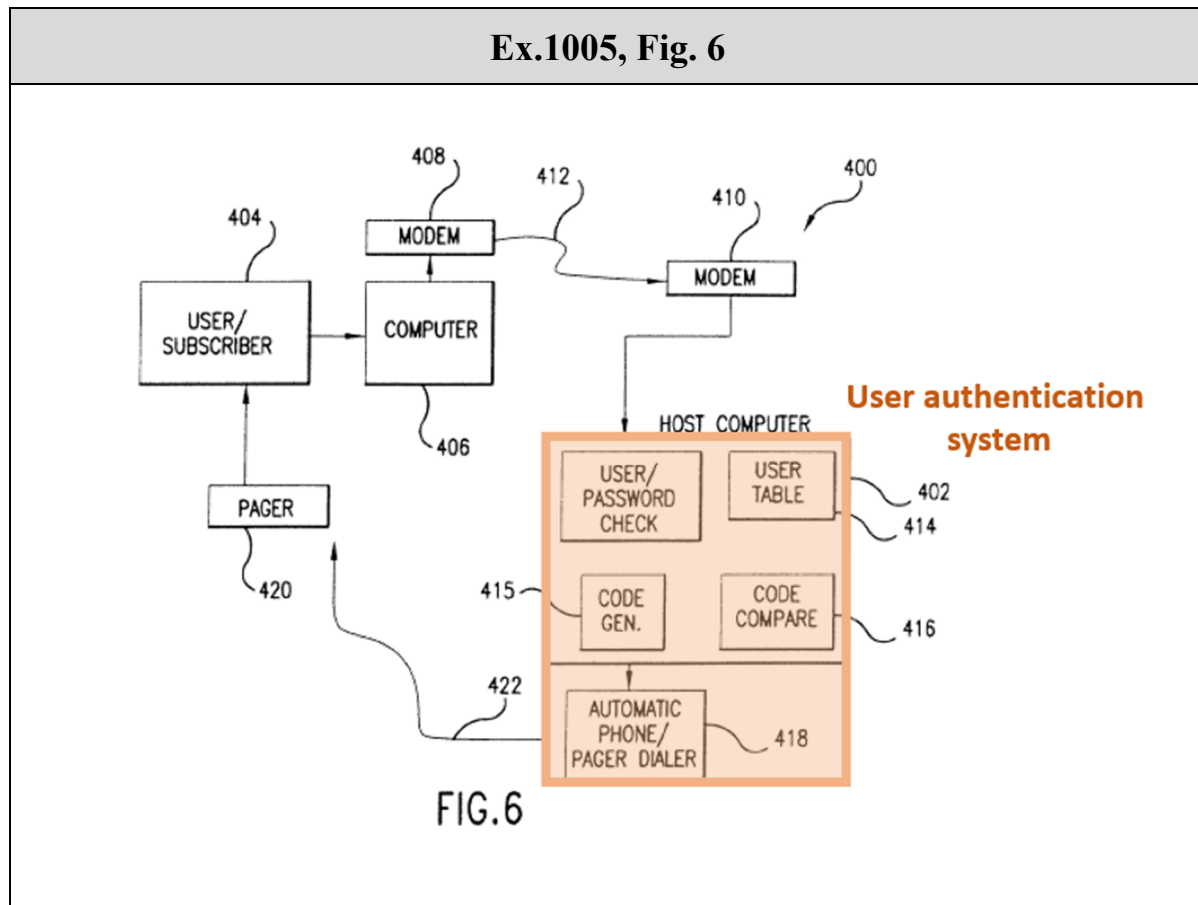
A. Claim 5

1. 5[pre]—“A user authentication system comprising:”

Veneklase discloses the preamble: “[s]everal embodiments of computer security systems [that] are adapted to grant an authorized individual access to a

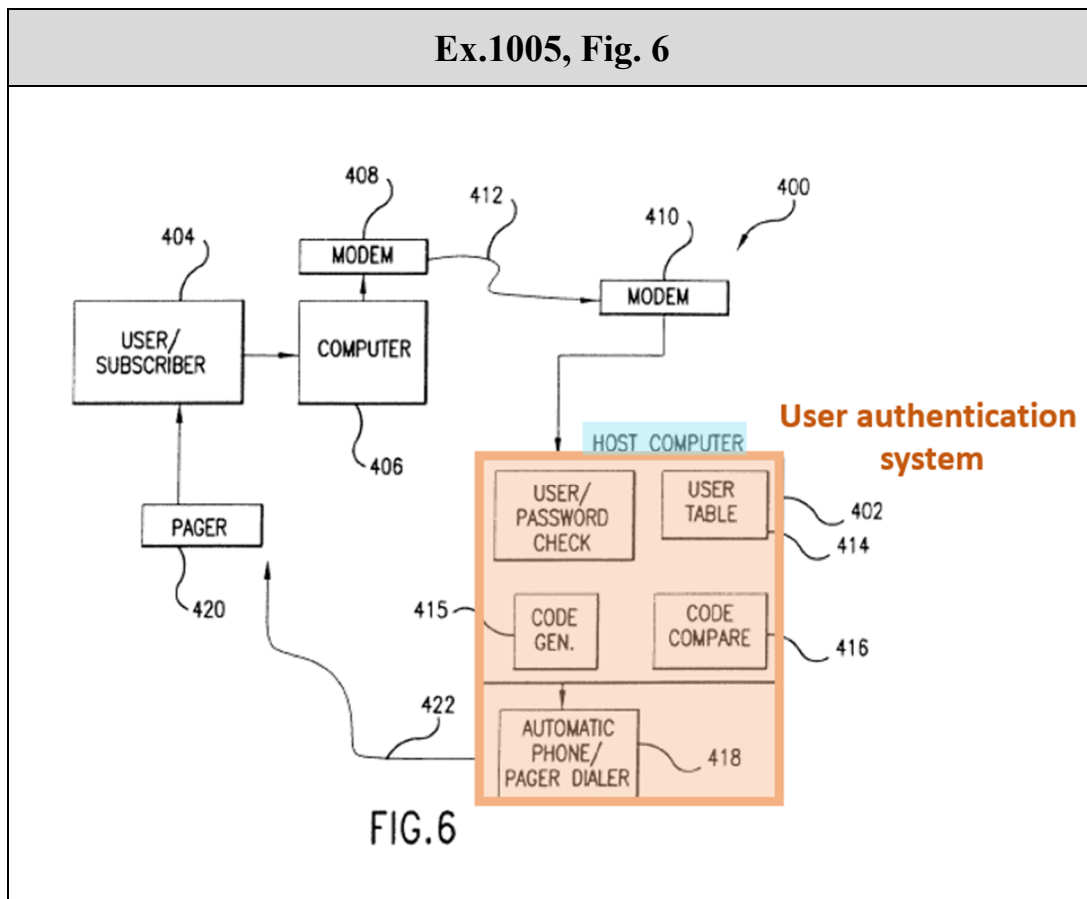
⁵ Claim 1 is a method claim with similar limitations to claim 5 and, like claim 7, requires that the system receive a token request from a user via a cell phone network.

secured domain, such as a computer or data stream.” Ex.1005, Abstract, Fig. 6;
Ex.1002, ¶¶64-66.



2. 5[a]—“a computer processor;”

Veneklas teaches this limitation. *Veneklas* discloses that its authentication system operates in host computer 402. Ex.1005, 7:29-8:27, Fig. 6. *Veneklas* further discloses that computer 80, which corresponds to computer 402, can “comprise a microprocessor.” *Id.*, 5:55-6:4, 7:34-39, Fig. 1; Ex.1002, ¶¶67-69.

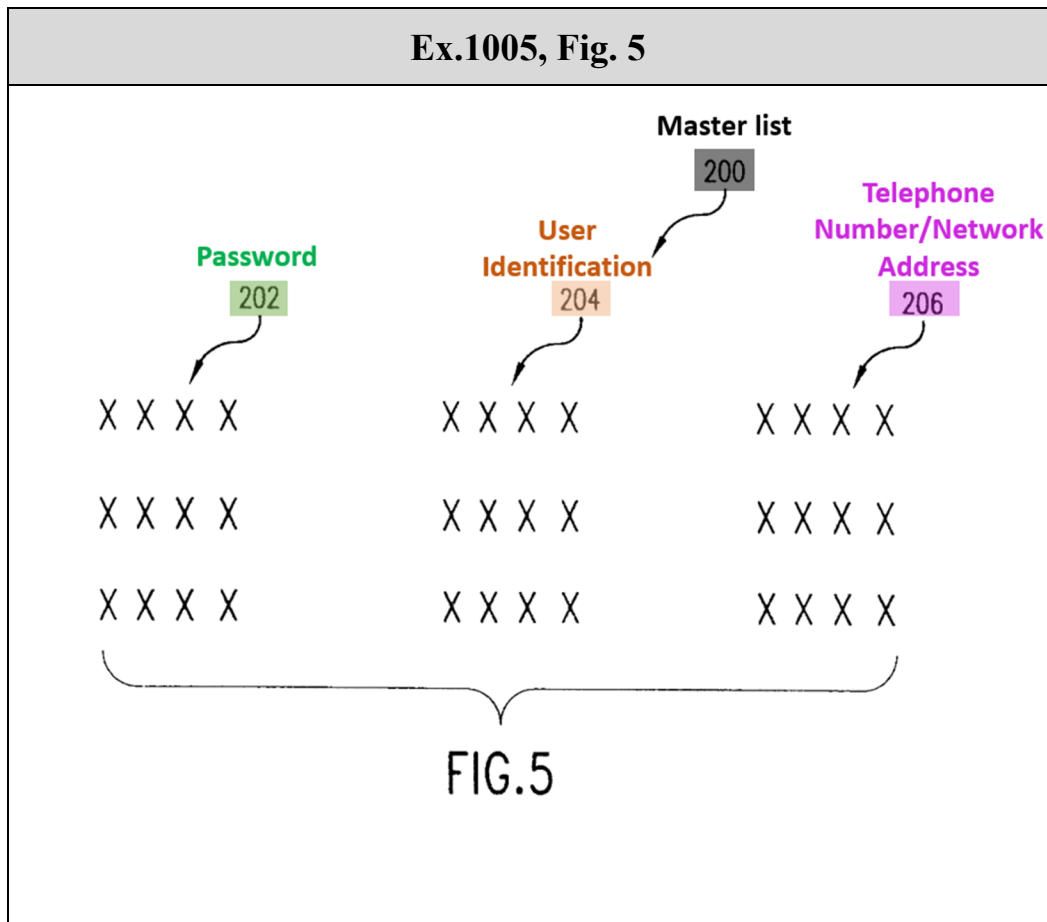


3. 5[b]—“a user database configured to associate a user with a personal communication device possessed by the user, said personal communication device configured to communicate over a cell phone network with the user authentication system;”

Venklase teaches or renders obvious this limitation. Ex.1002, ¶¶70-76.

Venklase discloses that “host computer 402 checks the received identification code and cross references the received password code against a pager phone number list resident within the user table 414” stored in computer 402. Ex.1005, 8:1-5, Fig.6. As shown in Figure 5, “each authorized password 202...has a unique first entry 204 associated with it and which **identifies the name of the authorized**

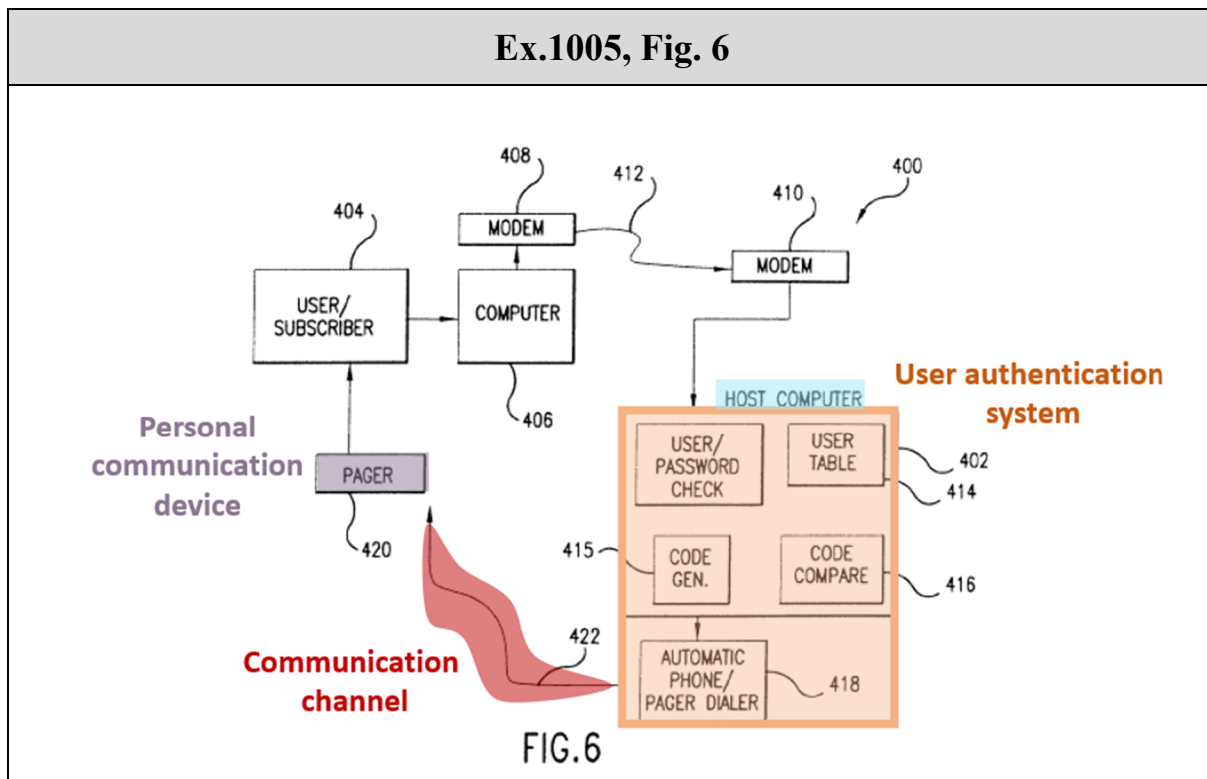
user who has been assigned that corresponding password and at least one telephone number 206 and/or network address associated with the identified user.” *Id.*, 6:15-26.



Veneklasė's association of a telephone number with user identification 204 and a personal communication device (e.g., a pager) is what the '658 Patent discloses. *Compare* Ex.1005, 8:1-5, *with* Ex.1001, 2:17-18. Upon determining that the received user identification 204 is matched with a telephone number, *Veneklasė's* “automatic dialer 418 telephones the conventional and commercially

available pager 420 by means of **conventional and commercially available communication channel 422.**” Ex.1005, 8:5-14.

Veneklase’s personal communication device (e.g., pager 420) is configured to communicate with the user authentication system (e.g., host computer 402) over a cell phone network (e.g., communication channel 422). See, Ex.1005, Fig. 6.



Veneklase explains that the communication channel over which the random code is sent could be a “**communications channel 84 [that] comprises a pager or cellular phone.**” *Id.*, 8:55-58. A POSITA would have understood that *Veneklase*’s “channel 422” discloses the claimed “cell phone network,” which the ’658 Patent explains includes networks that communicate with cell phones and/or

paggers. Ex.1002, ¶¶73-74; *see* Ex.1001, 5:32-40, Abstract, 1:10-11, 2:6-8, 2:28-31, 3:1-3, 4:13-17, 9:45-54.

To the extent it is argued that *Veneklase* does not disclose a cell phone network, a POSITA would have found it obvious to implement the authentication system of *Veneklase* using one. *Veneklase* explicitly contemplates using cell phones instead of paggers. Ex.1005, 8:55-58. *Veneklase* explains that utilizing “communications channel 84” to communicate with a cell phone could reduce the predetermined period before which a password would expire because use of a cell phone would allow the user to “ha[ve] immediate access to the code upon transmission.” *Id.* A POSITA would have recognized that this would increase security (*e.g.*, by reducing times during which a password could be stolen) and user convenience (*e.g.*, by displaying passwords instantaneously on cell phones that were already carried by users and have a wide range of functionality and often larger, easier-to-view screens). In addition, it would have been obvious to use a cell phone network to send *Veneklase*’s random code because doing so would be a simple substitution of one known element (*e.g.*, pager network) for another (*e.g.*, cell phone network) and would have made the system available to more users having different types of devices and in more locations, which is one of *Veneklase*’s objectives. Ex.1005, 1:15-49. A POSITA would have had a reasonable expectation of success in modifying *Veneklase*’s authentication system

to use a cellular network instead of a pager network because these networks operate similarly, often using the same protocols, such that the modification would have merely involved swapping out devices and making rudimentary software configuration changes. Ex.1002, ¶¶75-76.

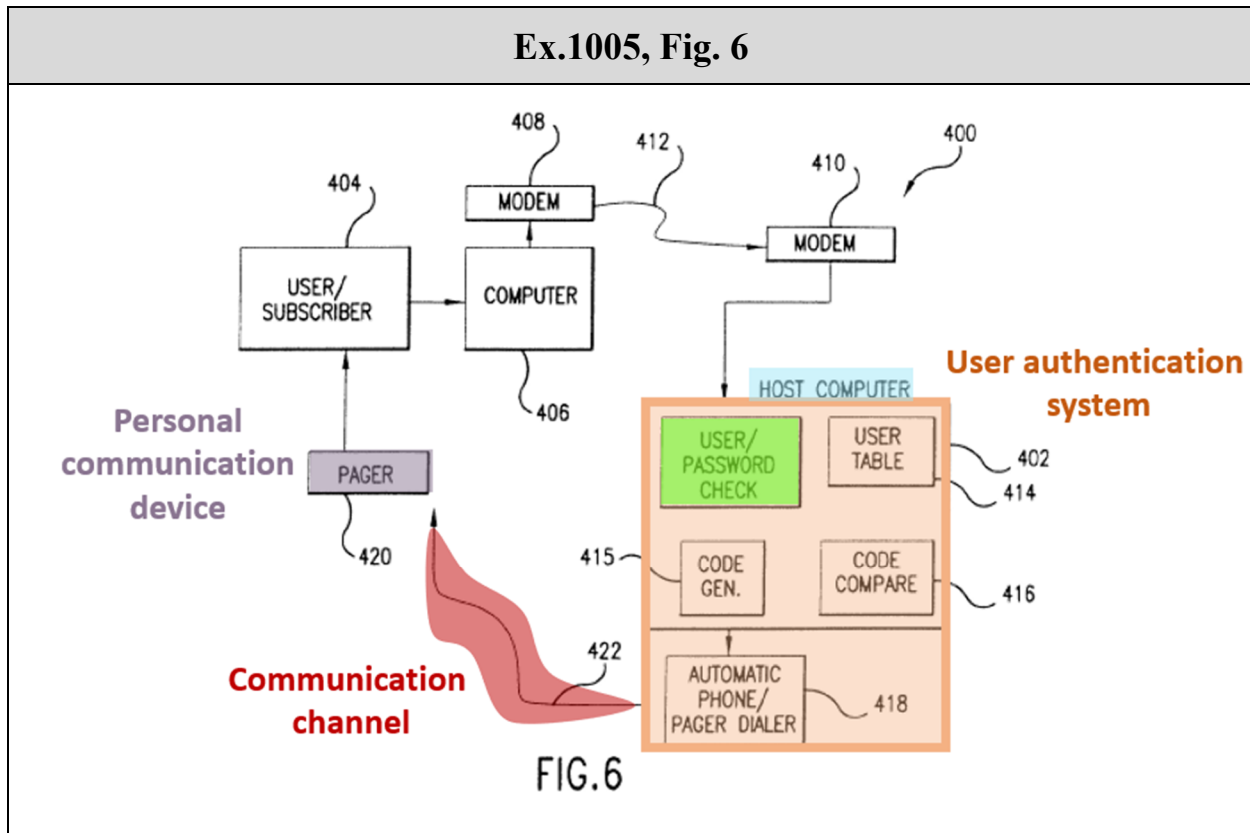
4. **5[c]—“a control module executed on the computer processor configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a password associated with the user to be the new password;”**

Veneklase in combination with *Jonsson* renders this limitation obvious.

Ex.1002, ¶¶77-84. *Veneklase* discloses “the steps of assigning a password to the user; receiving the password by use of a first communications channel; generating a code in response to the received password; transmitting the code by use of a second communications channel to the user; transmitting the code to the computer; and allowing access to the computer only after the code is transmitted to the computer.” Ex.1005, 4:8-15.

Veneklase discloses a “user/password check” module (*i.e.*, a control module) located on the host computer system 402 (*i.e.*, the computer processor). *See* Ex.1005, 7:55-8:5, Fig. 6; *see id.*, 6:10-14.⁶

⁶ The Unified IPR identified means-plus-function structure for “control module.” Ex.1012, 12-13. Out of an abundance of caution Petitioner identifies that same corresponding structure for purposes of this proceeding only. Ex.1001, 2:32-48, 8:2-8, 8:53-9:44, Figs. 1, 4, 5. As explained herein, that corresponding structure is present in the cited combination for the functional aspects, and the cited combination also includes “software executed on a ‘server’ that: (1) associates user ID with passcode and phone number of user’s personal communication device, (2) generates a new password, and (3) sets or rests the password associated with the user ID.” Ex.1002, ¶78.



This user/password check module assigns two passwords, one that is known to the user (“received password”) and one that is not previously known to the user. Ex.1005, 4:7-15. After the “received password” is entered by the user via the computer, the system “generate[s] a substantially random and/or pseudo-random number or code,” which is sent to the user’s mobile device and then input to the computer by the user. *Id.*, 6:27-33.

While *Veneklas* teaches an authentication system in which the user inputs both a token that is not known to the user beforehand (*e.g.*, random code) and a passcode that is known to the user (*e.g.*, received password), it does not disclose creating a new password based on those two items. However, it would have been

obvious to combine those two steps and create a new password based on both items, for example by incorporating *Jonsson*'s teachings of a combined submission to apply to *Veneklase*'s random code and received passcode.

Jonsson discloses a system that includes a service node that “generates a challenge code and requests that the challenge code be sent to the personal unit 20 via an authentication challenge network 28.” Ex.1006, 4:24-5:6, 9:9-25. The challenge code is a token because it is not previously known to the user. Additionally, *Jonsson* discloses the use of a “user input such as a personal identification number (PIN),” which is already known to the user. *See* Ex.1006, 3:3-10, 3:14-18, 7:32-8:11; Ex.1002, ¶¶79-82.

In *Jonsson*, an algorithm “**calculates a response code [*i.e.*, claimed new password] based on the received challenge code [*i.e.*, claimed token], the user input (e.g., PIN) [*i.e.*, claimed passcode], and optionally the secret key.” Ex.1006, 8:12-14, 7:5-10, 9:23-25. “[F]or a correct response code to be generated, the challenge code, the user input and the secret key (if used) have to be in accordance with the expectations of the service node 26 or authentication center 30 if access to the service is to be granted.” *Id.*, 8:14-18. “This provides a triple check on the identity of the user, requiring information from three separate sources (user: PIN, service node or authentication center: challenge code, and provider of**

the personal unit: secret key), thereby increasing the relative security of the transaction against fraud or other unauthorized use.” *Id.*, 7:18-23.

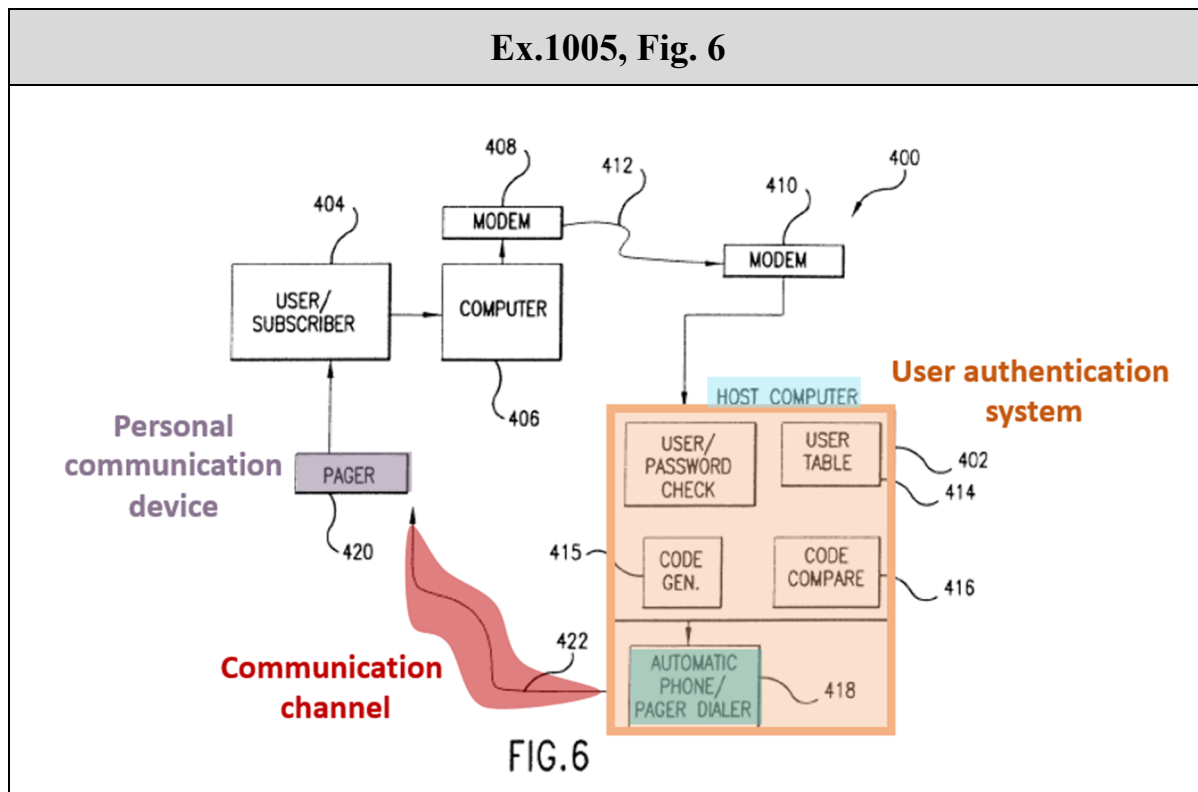
Additionally, *Jonsson* discloses that “[t]he response code is compared to an **expected response code [i.e., a created new password], which, in exemplary embodiments, may be pre-stored [i.e., set as the new password]** or generated using the same algorithm and variables.” *Id.*, 10:2-5. “The response code is to be **unique to each transaction,**” and a POSITA would have understood that this pre-stored expected response code is a new password associated with the user. *Id.*, 7:34-35; Ex.1002, ¶¶82-83; Ex.1004, 195-96 (applicant traversing prior art for not having a response code that is unique to each transaction).

In combination, the authentication system in *Veneklase* would incorporate *Jonsson*’s teachings to use an algorithm to create a new password (*e.g.*, *Jonsson*’s response code/*Veneklase*’s combined received password and random code in view of *Jonsson*’s teaching) based on a known passcode (*e.g.*, *Veneklase*’s received password/*Jonsson*’s PIN) and an unknown token (*e.g.*, *Veneklase*’s random code/*Jonsson*’s challenge code). Ex.1002, ¶84.

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

Veneklase teaches or renders obvious this limitation. Ex.1002, ¶¶85-87. As explained above in Section IX.A.3, incorporated here, *Veneklase*’s communication

channel 422 discloses or renders obvious the claimed cell phone network. After *Veneklase*'s system correlates an identification code with a user's phone number, a random number code is generated and passed to the phone/pager dialer 418 which transmits the code to the personal communication device through communication channel 422. Ex.1005, 7:52-8:17, Fig. 6.



A POSITA would have recognized that *Veneklase*'s automatic phone/pager discloses the claimed communication module, and that the claimed cell phone network can support both pagers and cellular phones. See Ex.1001, 10:31-34 ("the

communication module 118 is a phone dialer 622”), 5:32-40, Abstract, 1:10-11, 2:6-8, 2:28-31, 3:1-3, 4:13-17, 9:45-54; Ex.1002, ¶¶86-87.⁷

6. 5[e]—“**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,**”

Veneklase, alone or in combination with *Jonsson*, teaches or renders obvious this limitation. Ex.1002, ¶¶88-92. *Veneklase* discloses an authentication module (e.g., code compare module 416) configured to receive the password from the user through a secure computer network (e.g., receiving the random code via communication channel 412). Specifically, *Veneklase* discloses that “user 404 now enters the code he or she has received from the pager 420...and **sends this password or pseudo-random code back to computer 402 where it is compared**

⁷ The Unified IPR identified means-plus-function structure for “communication module.” Ex.1012, 13. Out of an abundance of caution Petitioner identifies that same structure for purposes of this proceeding only. Ex.1001, 2:39-42, 5:66-6:1, 6:18-20, 10:14-41, Fig. 1. As explained herein, that structure is present in the cited combination for the functional aspects, and the cited combination also includes a “(1) a mobile device with messaging capabilities, (2) a phone dialer, or (3) a connection card connected to a messaging service provider.”

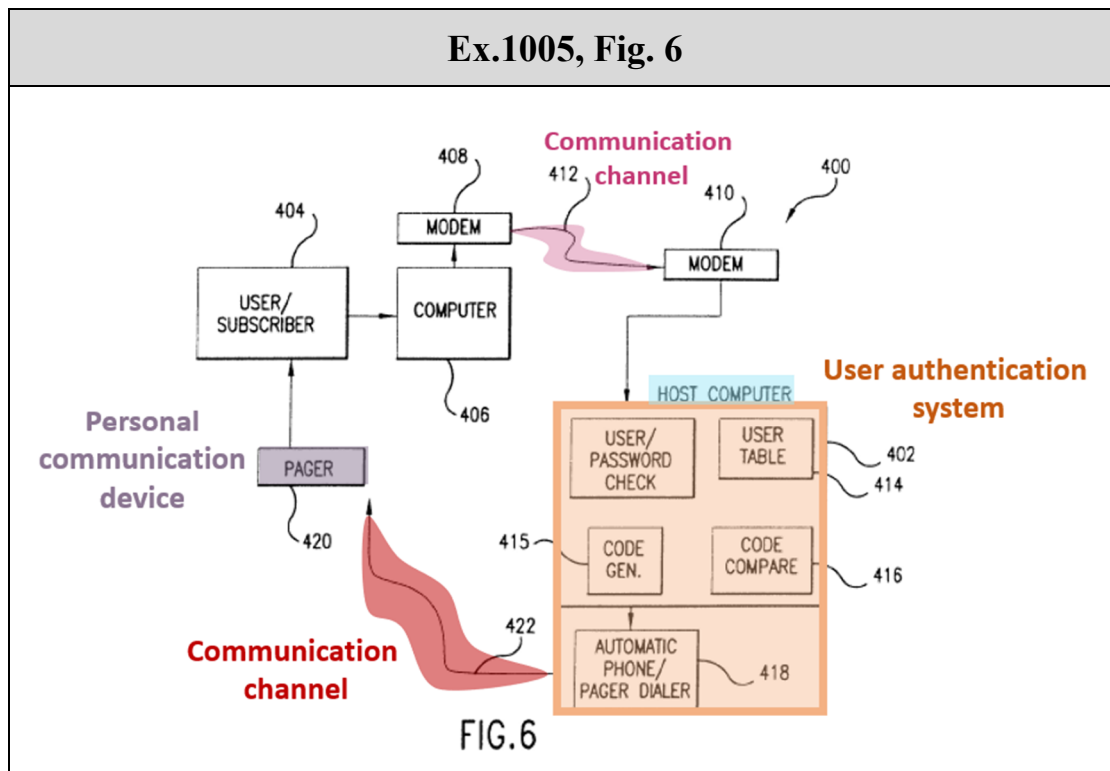
within the software subroutine module denoted as ‘code compare’ 416.”

Ex.1005, 8:18-27, 3:50-4:3. “[A]ccess to the computer system [is allowed] only if th[e] individual generates and communicates the code to the code generation means.” *Id.*, 4:1-3.

In combination with *Jonsson*, a POSITA would have understood that the new password (*i.e.*, *Jonsson*’s response code/*Veneklase*’s combined received password and random code in view of *Jonsson*’s teaching) being sent back to computer 402 and compared against the expected response code is the one created by the algorithm based on both the known passcode (*i.e.*, *Veneklase*’s received password/*Jonsson*’s PIN) and the randomly generated token (*i.e.*, *Veneklase*’s random code/*Jonsson*’s challenge code). Ex.1002, ¶¶88-89.⁸

⁸ The Unified IPR identified means-plus-function structure for “authentication module.” Ex.1012, 13-14. Out of an abundance of caution Petitioner also identifies that same structure for purposes of this proceeding only. Ex.1001, 3:4-25, 5:3-10. Fig. 1. As explained herein, that structure is present in the cited combination for the functional aspects, and the cited combination also includes “software executed on a ‘server’ that: (1) receives a submitted password in response to a request for authentication and (2) grants access to the user if the submitted password matches the valid password.”

Veneklas also discloses that the channel through which the user submits credentials to the host computer and the initial sending of the random code to the personal device “**utilize[] two distinct communications channels.**” Ex.1005, 7:11-28, 3:50-4:3. Specifically, *Veneklas*’s “typical communications channel (e.g., a conventional ‘dial-up’ telephone line) 412” (*id.*, 7:29-51) is distinct from the “communication channel 422 (e.g. voice line) [that] transmits the code to the user’s pager.” *Id.*, 8:11-17, Fig. 6 (showing distinct communication channels 412 and 422).



A POSITA would have understood that the network including communication channel 412 is a secure computer network because of the

authentication procedures employed in *Veneklase*. See *id.*, 9:3-14 (describing host computer on the network as “the secure domain”); Ex.1002, ¶¶90-92. This corresponds to what the ’658 Patent describes as a secure computer network. See Ex.1001, 1:63-65, 2:49-3:3, 4:9-26, 10:30-41.

7. **5[f]—“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 a secure computer network.”**

Veneklase, in combination with *Jonsson*, renders obvious this limitation.
Ex.1002, ¶¶93-100.

Activates Access – Unified IPR Board’s Construction. The Board in the Unified IPR rejected Petitioner’s arguments and stated that “Claim 5 ...does not require that the account be activated in response to creation of the password.” Ex.1013 (Unified Institution Decision), Paper 9 at 24. *Veneklase* discloses wherein the authentication module (*e.g.*, code compare module 416) activates access to the account in response to the password (*e.g.*, allows access if the random codes match). Specifically, *Veneklase* discloses that the user “sends this password or pseudo-random code back to computer 402 where it is **compared within the software subroutine module denoted as ‘code compare’ 416** in Figure 6” and,

“[i]f the comparison yields a match, the user 404 is allowed access to computer 402 and/or to a portion of computer 402.” Ex.1005, 8:18-27, 6:45-7:10.

Activates Access – District Court’s Construction. Judge Payne construed this phrase to mean “activates access to the account in response to the creation of the password.” Ex.1011, 16.⁹ To the extent the Board adopts this construction, *Veneklase* in view of *Jonsson* still render this limitation obvious. As discussed above, *Jonsson* discloses creating “an **expected response code [i.e., a created new password], which, in exemplary embodiments, may be pre-stored [i.e., set as the new password]** or generated using the same algorithm and variables.”

Ex.1006, 10:2-5. *Jonsson* explains that “[t]he response code is to be **unique to each transaction,**” and a POSITA would have understood that this pre-stored expected response code is a new password associated with the user. *Id.*, 7:34-35.

A POSITA would have recognized that it would have been obvious to activate access to the account in response to *Jonsson*’s generation and storage of the expected response code so as to enable a user to readily access their account after they were verified as the sole requester of that response code. At a minimum, this would have been obvious to try for the simple reason that it was one of a finite

⁹ For the purposes of this proceeding, Petitioner asserts that this phrase should be construed according to the District Court’s construction.

number of options, i.e., whether to immediately activate an account in response to the expected response code or wait a period of time before activating the account. Ex.1002, ¶¶94-95.

In addition, *Veneklase* discloses that the user has an account on the secure computer network (e.g., the user's password in the master password list corresponds to user's account). Specifically, *Veneklase* discloses that this system is accessible only when the password is found within the master password list. Ex.1005, 6:15-26 (“[E]ach authorized password 202, contained in this master password list 200, has a unique first entry 204 associated with it and which identifies the name of the authorized user...”). A POSITA would therefore have understood that for the password associated with the authorized user to appear in the list, that user must have an account on the secure computer network. Ex.1002, ¶¶96.

Veneklase also discloses that its system 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. Specifically, *Veneklase* “includes a timer or ‘timing means’ 40” that can “operate and/or execute within and/or upon computer 80,” such as a watchdog timer. Ex.1005, 8:28-39. 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. *Id.*, 8:40-49. “If the second password [sent to the cellular phone] was not received within the predetermined period of time, analyzing means 12 denies entry to the secured domain (e.g., computer 80).” *Id.*, 9:3-6. A POSITA would have understood that this denial of entry to the secured domain (*i.e.*, deactivating of the account) occurs regardless of whether the user might know or guess the correct password (since the reference teaches that once the predetermined period of time expires, entry is denied and there are no caveats to that denial of entry), and thus **said account is not accessible through any password via the secure computer network**. Ex.1002, ¶¶97.

In combination with *Jonsson*, a POSITA would have understood that the new password (*e.g.*, response code) being sent back to computer 402 and compared against the expected response code is the one created by the algorithm based on both the known passcode (*e.g.*, PIN) and the randomly generated token (*e.g.*, challenge code). The predetermined period would thus be the time allowed after generation of the expected response code and/or of the new password 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. *Id.*

Veneklase discloses the claimed deactivating limitation because the teaching is nearly identical to how this limitation is described in the '658 Patent. *See* Ex.1001, Fig. 5, 9:61-64; Ex.1002, ¶¶98-100.

B. Ample Motivation Existed to Combine *Veneklase* and *Jonsson*

A POSITA would have been motivated to incorporate *Jonsson*'s teachings related to an authentication system in which a password is created based on known and unknown inputs into *Veneklase*'s authentication system that utilizes both a known password and an unknown random code. Ex.1002, ¶¶101.

First, a POSITA would have appreciated that *Veneklase* and *Jonsson* are in the same field of endeavor and address similar problems as each other and the '658 Patent. *See* Ex.1001, 1:7-11 (describing “authentication of users of secure systems...through personal communication devices”). *Veneklase* discloses “computer security systems...which are adapted to grant an authorized individual access to a secured domain” by use of a pager. Ex.1005, Abstract. *Jonsson* discloses “[a]uthorization for...a service is provided by a modified pager.” Ex.1006, Abstract.

Veneklase and *Jonsson* are particularly pertinent to the '658 Patent's teachings of authenticating user access by “using a device that many users already

carry,” *e.g.*, “a mobile phone or a pager.” Ex.1001, 1:56-59. *Veneklase* discloses the same solution of using a mobile device for authentication. Ex.1005, 8:5-15. *Jonsson* likewise avoids the shortcomings of prior art systems “requir[ing] specially equipped, and often dedicated, terminals, which raises the cost and reduces the availability of the associated electronic service.” Ex.1006, 2:8-14. Ex.1002, ¶¶102-103.

Second, 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. *Veneklase* teaches a system in which a user inputs a password known beforehand; receives a randomly generated, previously unknown code; and then inputs that for authentication purposes. *See* Ex.1005, 7:52-8:27. *Jonsson* discloses a similar authentication system that involves the user inputting a known PIN. *See* Ex.1006, 10:22-31. *Jonsson* discloses an algorithm that “calculates a response code based on the received challenge code, [and] the user input (*e.g.*, PIN).” *Id.*, 8:12-14. *Veneklase*’s system allows for authentication through user input of a known and unknown code at separate times through the secure computer network in a two-step process, and a POSITA would look to *Jonsson* for the added benefit of 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. Ex.1002, ¶¶104.

Third, 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. Ex.1002, ¶¶105 (explaining SIM swapping); Ex.1006, 2:30-3:18.

Fourth, *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. See Ex.1005, 9:26-10:11. Thus, a POSITA would have been motivated to use an algorithm for creating a new password based on the known password and the previously unknown randomly generated code, as described in *Jonsson*, for additional security. Ex.1002, ¶¶106.

While *Veneklase* mentions certain weaknesses of encryption algorithms as background, this is in the context of “modifying and/or changing the transmitted data in a certain manner, and/or requiring the transmission and receipt of modified data before access is granted.” Ex.1005, 2:37-56. These drawbacks would not apply in the context of the algorithm for creating a new password disclosed in

Jonsson because it would not “provide[] all of the transmitted data, in some form.” *Id.*; Ex.1006, 10:22-27. In other words, the drawbacks noted in *Veneklase* are directed to encrypting all transmitted data as compared to using encryption to create a new password to access the data. Additionally, the combination would still utilize all of the protections provided for in *Veneklase*, so it only provides additional security (not less). Finally, *Jonsson* clearly discloses that “[t]he specific algorithm used in a given embodiment is not germane to the present invention,” and “[a]lgorithms of this type are known in the art” (Ex.1006, 7:10-14), so a POSITA would not have been concerned about their cost or complexity. Ex.1002, ¶¶107-108. In addition, the Federal Circuit has stated that “[a] reference that ‘merely expresses a general preference for an alternative invention but does not criticize, discredit, or otherwise discourage investigation into’ the claimed invention does not teach away.” *Meiresonne v. Google, Inc.*, 849 F.3d 1379, 1382 (Fed. Cir. 2017).

Lastly, a POSITA would have been motivated to utilize the algorithm of *Jonsson* in the system of *Veneklase* because it would have been used in the same way, *i.e.*, to provide another layer of security. Ex.1006, 7:5-17. *Veneklase* discloses the use of known passwords and previously unknown randomly generated codes, so it would have been obvious for a POSITA to combine the two inputs. Ex.1002, ¶¶109.

A POSITA would have had a reasonable expectation of success modifying *Veneklase*'s authentication system, which requires the use of both a known password and a previously unknown randomly generated code, to create a new password based on those two values, as taught by *Jonsson*, because doing so would have merely made two steps into one without requiring any additional hardware (or alternatively *Jonsson*'s PIN and generated response code could also have been easily incorporated into *Veneklase*'s system). Therefore, a POSITA would have been motivated to combine, and would have had a reasonable expectation of success in combining, *Veneklase*'s teachings, including a control module executed on the computer processor configured to create a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, with *Jonsson*'s teaching related to creating and setting a new password based at least upon the token. Ex.1002, ¶¶110.

C. Claim 6

Claim 6 depends from claim 5, which is obvious in view of *Veneklase* and *Jonsson* as discussed above in Section IX.A, incorporated herein. Claim 6 adds: “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.”

Veneklase in combination with *Jonsson* renders this limitation obvious.

Ex.1002, ¶¶111-15. *Veneklase* discloses a user/password check module (*i.e.*, a control module), and 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 (*e.g.*, generating a code in response to the received password).

Ex.1005, 7:55-8:5, Fig. 6, 4:7-12. While *Veneklase* does not expressly disclose that the control module is configured to create a new password in response to the user's request, it would have been obvious to a POSITA to modify this module to perform that function.

A POSITA would look to a reference such as *Jonsson*, which discloses a similar authentication system that is further configured to receive a request from the user for the token (*i.e.*, the service node receives the user's request and then generates a token or challenge code in the node or an authentication center) and to create the new password in response to the request (*i.e.*, the expected response code used for the comparison). Ex.1006, 9:2-7, 10:2-5. Specifically, *Jonsson* discloses that the user requests "access through terminal 22 by transmitting the request over a service access network 24 to a service node 26." *Id.*, 9:2-4. In response, the service node generates a token or challenge code that is "sent over an authentication challenge network 28 to the personal unit." *Id.*, 9:5-8. When a response code is generated by the personal unit, displayed to the user, and then

input by the user into terminal 22, it is “compared to an expected response code” that was “pre-stored or generated using the same algorithm and variables” in the service node or authentication center. *Id.*, 10:2-5. A POSITA would have understood that the new response code being compared is a new password because the “response code is to be unique to each transaction.” *Id.*, 7:34-35; Ex.1002, ¶¶112-114.

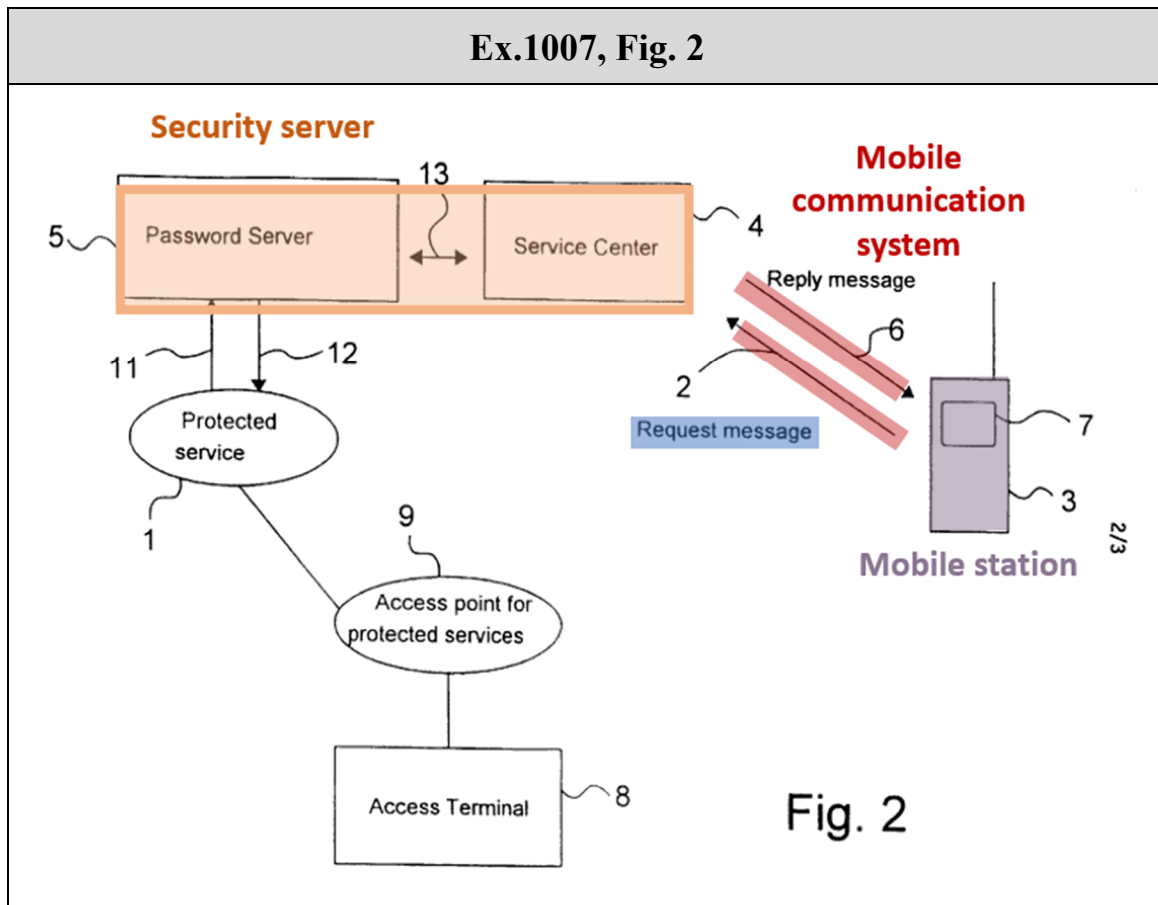
In combination, *Veneklase*’s authentication system would incorporate *Jonsson*’s teachings related to using an algorithm to create a new password (*e.g.*, response code) following a user’s request for a token (*e.g.*, random code/challenge code). Thus, *Veneklase* in combination with *Jonsson* teaches wherein the communication module (*e.g.*, user/password check module) is further configured to receive a request from the user for the token (*e.g.*, random code/challenge code), and wherein the control module is further configured to create the new password in response to the request (*e.g.*, response code). Ex.1002, ¶115.

D. Claim 7

Claim 7 depends from claim 6, which is obvious in view of *Veneklase* and *Jonsson* as discussed in Section IX.C, incorporated herein. Claim 7 adds: “wherein the request is transmitted by the user through the personal communication device.”

Claim 7 is rendered obvious by *Veneklase* in view of *Jonsson* and *Sormunen*. Ex.1002, ¶¶116-120. Specifically, *Sormunen* discloses that in order to obtain a

password or list of passwords, “the user of the service **sends a short message 2** from a paging terminal 3, such as a mobile station.” Ex.1007, 5:35-38, Fig. 2.



Sormunen discloses that “the **short message 2** includes a password request.” *Id.*, 5:38-6:1. In the *Veneklase-Jonsson* system described above, a POSITA would have understood that this request would be for a token (e.g., random code/challenge code).

Sormunen’s “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. *Sormunen* notes that “[t]he present invention can be applied especially in such telecommunication systems in which it is possible to transmit short messages...on the basis of a terminal key, such as a telephone number,” and that “[t]his quality is included in mobile communication systems” such as “a **cellular system, a paging system, and a mobile phone system.**” *Id.*, 4:30-5:8. Ex.1002, ¶¶117-19.

Ample motivation existed for a POSITA to incorporate *Sormunen*’s teachings related to an authentication system in which a personal communication device (*e.g.*, mobile phone) communicates with the authentication system via a cellular network (*e.g.*, GSM system) in combination with *Veneklase* and *Jonsson*. A POSITA would have recognized that by incorporating *Sormunen*’s teachings, the authentication systems in *Veneklase* and *Jonsson* could be operated on the well-known and ubiquitous GSM system. Ex.1002, ¶120. Both *Veneklase* and *Jonsson* disclose using conventional communications channels for sending a user’s request for a token. *See* Ex.1005, 7:39-45 (disclosing using “typical communications channel”); Ex.1006, 5:27-30 (disclosing using “any communication system, such as...cellular radio telephone network”), 9:2-4.

E. Ample Motivation Existed to Combine *Veneklase*, *Jonsson*, and *Sormunen*

First, as explained in Section IX.B, incorporated here, *Veneklase* and *Jonsson* are analogous to the '658 Patent. *Sormunen* is similarly analogous. *Sormunen* discloses a “for obtaining at least one item of user specific data...at least partly by using paging or a short message service.” Ex.1007, Abstract. Like *Veneklase* and *Jonsson*, *Sormunen* is also pertinent to the '658 Patent's teachings by solving the same problem by transmitting authentication information to the user via a mobile network. Ex.1007, 4:30-5:8; Ex.1002, ¶¶121-23.

Second, a POSITA would have been motivated to combine the three references because such a combination would be commercially desirable and obvious to try. Ex.1002, ¶124. Indeed, *Sormunen* teaches the use of conventional mobile communication systems, *e.g.*, the well-known GSM system. Ex.1007, 5:1-3. *Veneklase* likewise advocates for a “typical communications channel,” noting the benefits of being “relatively low-cost, but effective” and “very cost effective as it employs substantially ‘off the shelf’ and readily available components.” Ex.1005, 7:13, 7:17-24, 7:44-45. *Jonsson*'s teachings similarly rely on conventional cell phone technology: “the capacity for performing the necessary calculations exists in conventional cellular telephones...allowing the present invention to be implemented through software.” Ex.1006, 7:24-31.

In view of *Veneklase*'s advantages of being "very cost effective" and "readily available," it would have been obvious for a POSITA to further modify *Veneklase* by implementing its system using a conventional cellular system (e.g., GSM), as taught by *Sormunen*, to make it widely accessible to mobile phone users. A POSITA would recognize that by doing so, 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* Ex.1007, 5:12-18 ("[a] further advantage of the fast data transmission is that...security may thus be improved"). Thus, a POSITA would have been motivated to combine *Veneklase*, *Jonsson*, and *Sormunen* in order to maximize the accessibility, performance, efficiencies, and security offered by the systems and methods disclosed in each reference. Ex.1002, ¶125.

Third, a POSITA would have recognized that adding *Sormunen*'s functionality for a user to request a token via their mobile phone would make the authentication process more convenient and easier to use without compromising security. Specifically, adding *Sormunen*'s functionality that enables a user to submit the token request from the same personal device to which the token will be sent ensures that the user knows—and already has in their hand—the device to which the token will be sent and that the user will be able to see and input the

token before it expires. Indeed, instead of requesting a token from a computer terminal and sending it to a device that the user has potentially misplaced or cannot readily locate, the *Veneklase-Jonsson* system as modified by *Sormunen* would allow that user to simply request the token from a device they may already have at hand and are using. This would enhance the user-friendliness and convenience of the system and provide desirable and marketable features. This modification would not sacrifice the security of the system because, as discussed above, *Veneklase* discloses maintaining a master database that correlates the user's mobile number with other identifying and password information. The *Veneklase-Jonsson-Sormunen* system would therefore utilize *Veneklase*'s database to confirm that the request came from the appropriate phone number before providing any token in response. In fact, 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. Ex.1002, ¶¶126-27.

Fourth, a POSITA would have been motivated to combine these references because adding *Sormunen*'s token-request functionality merely applies known techniques to improve similar systems and devices. For example, *Sormunen* discloses that its token-request functionality could be implemented with the

already-existing cellular system described in *Veneklase* and *Jonsson*. See Ex.1007, 4:30-5:8; Ex.1005, 6:37-44; Ex.1006, 5:27-35. A POSITA would have recognized that this implementation would merely involve applying known techniques to modify mobile phone software to allow a user to transmit a token request over a cellular system and to modify system software to receive and recognize that request. A POSITA would have recognized that such an implementation would be readily achieved and work successfully without any modifications to system or device hardware. Ex.1002, ¶128.

Therefore, a POSITA would have been motivated to modify, and would have had a reasonable expectation of success in modifying, *Veneklase*'s authentication system with *Jonsson*'s teachings related to its algorithm and *Sormunen*'s teachings related to the transmission of token requests over a cellular network. Ex.1002, ¶129.

X. GROUND #2: CLAIM 2 IS OBVIOUS OVER VENEKLASE IN VIEW OF JONSSON, SORMUNEN, AND KAUFMAN

Claim 2 depends from claim 1, which is rendered obvious by the combination of *Veneklase*, *Jonsson*, *Sormunen*, and *Kaufman*. Ex.1002, ¶¶130-150.

A. Claim 1

As shown in the chart below, and with the exception of limitation 1[b], claim 1 recites limitations analogous in scope to those of claim 5. The corresponding sections referenced in the chart below are incorporated by reference herein.

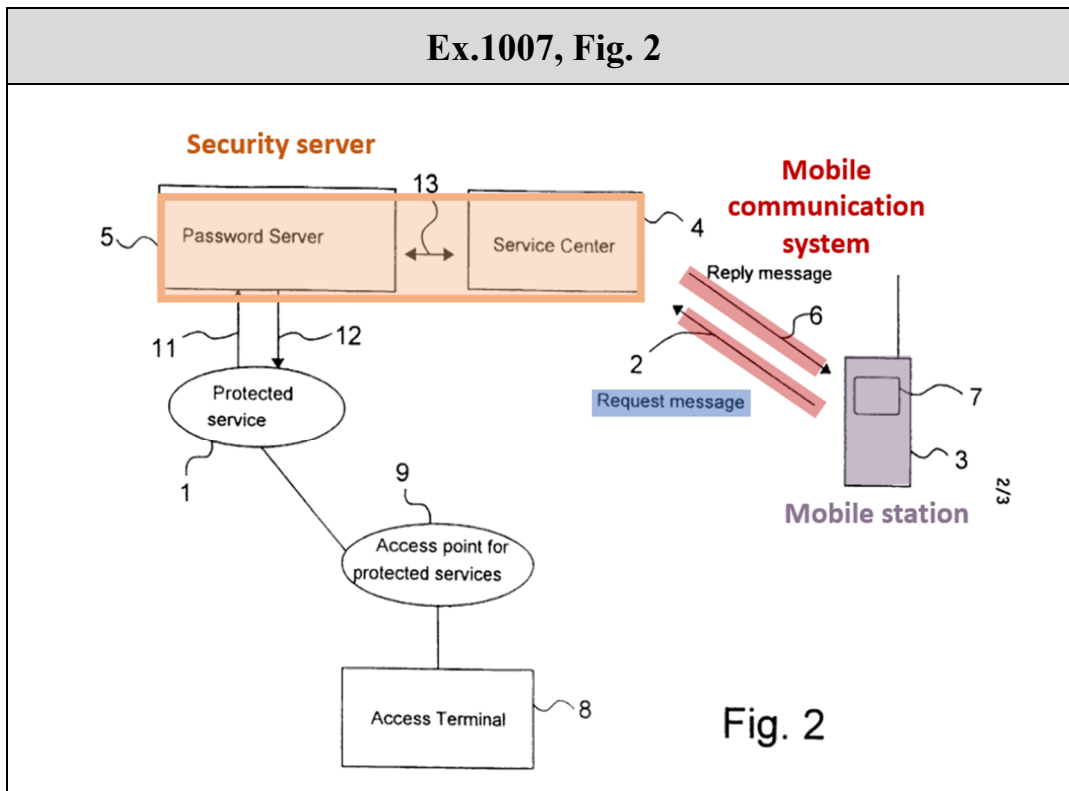
Claim 1 Limitation	Corresponding Analogous Claim 5 Limitation(s)	Section(s) Incorporated By Reference
1[pre]	5[pre], 5[e], 5[f]	IX.A.1, IX.A.6, IX.A.7
1[a]	5[b], 5[e]	IX.A.3, IX.A.6
1[b]	<i>See Claim 7 and below</i>	<i>See IX.D</i>
1[c]	5[c]	IX.A.4
1[d]	5[c]	IX.A.4
1[e] ¹⁰	5[f]	IX.A.7
1[f]	5[d]	IX.A.5
1[g]	5[e]	IX.A.6
1[h]	5[f]	IX.A.7

- 1. 1[b]—“receiving a request from the user for a token via the personal communication device, over the second network;”**

Veneklase in combination with *Jonsson* and *Sormunen* renders obvious this limitation. Ex.1002, ¶¶132-36. *Sormunen* discloses that in order to obtain a password, “**the user of the service sends a short message 2 from the paging**

¹⁰ The district court did not construe the “activating access” limitation in claim 1[e] the same as the “activates access” limitation in claim 5[f]. This limitation is rendered obvious as discussed with respect to the section titled “Unified IPR Board Construction” in Section IX.A.7.

terminal 3, such as a mobile station.” Ex.1007, 5:35-38, Fig. 2. “[T]he short message 2 includes a **password request.**” *Id.*, 5:38-6:1.



Sormunen’s “paging service center 4 processes the incoming message” and communicates with password server 5, which “forms a reply message containing one or more passwords and the user name in case a new user is registered.” *Id.*, 6:20-24.

Sormunen’s system can be utilized in “telecommunication systems in which it is possible to transmit short messages,” for example, “mobile communication systems includ[ing] [] a **cellular system, a paging system, and a mobile phone system.**” *Id.*, 4:30-5:8; *see id.*, claim 11.

A POSITA would have understood that a password request from *Sormunen*'s mobile request system would be for a token (*e.g.*, randomly generated challenge code) in accordance with the combined *Veneklase* and *Jonsson* system described with respect to claims 5-7. Ex.1002, ¶¶133-35.

Thus, *Veneklase* in combination with *Jonsson* and *Sormunen* discloses receiving a request (*e.g.*, a password request) from the user for a token (*e.g.*, randomly generated challenge code) via the personal communication device (*e.g.*, receiver unit/paging terminal), over the second network (*e.g.*, cellular network). Ex.1002, ¶136.

B. Claim 2

Claim 2 further requires “wherein the new password is generated by concatenating the token and the passcode.” *Veneklase* in view of *Jonsson*, *Sormunen*, and *Kaufman* renders this limitation obvious. Ex.1002, ¶¶137-141.

As discussed above, *Kaufman* discloses a system utilizing a password and a token, where “workstation 516 **computes a ‘transmission code’ based upon the password and the token.**” Ex.1008, 9:39-42. *Kaufman*'s “transmission code is calculated by using a first ‘hashing algorithm.’” *Id.* *Kaufman*'s “hashing algorithm” is “a one-way routine for transmuting multiple input data items, [that] **concatenat[es] selected items of the input data** and perform[s] a ‘hashing equation’ upon one or more items of the input data, in a specified order.” *Id.*, 9:43-

46. The disclosed “hashing equation” can “include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence.” *Id.*, 9:47-51; Ex.1002, ¶138.

Kaufman discloses different hashing algorithms that may be used to concatenate tokens and passcodes:

[H]ashing algorithm 1.0, explained more fully, comprises the following operations: the password is modified by the selected hashing equation, the **modified password is concatenated onto the token to form a concatenation**, and this concatenation is modified by the hashing equation. The system may be designed so that a specified single hashing algorithm, such as one of the algorithms 1.0-1.3, is used at all times;....

Ex.1008, 10:7-17. *Kaufman* explains that, in connection with the Table presented in the specification, reproduced below, “the ‘|’ symbol represents the concatenation operation.” *Id.*, 10:6-7.

Ex.1008, Hashing Algorithms Disclosed in <i>Kaufman</i>	
[1.0]	hash(token hash(password))
[1.1]	hash(hash(password token)
[1.2]	hash(token password)
[1.3]	hash(password token)

Id., 9:65-10:5.

A POSITA would also appreciate that Kaufman's system is the same as the one claimed in the '658 Patent. *See* Ex.1001, 4:52-53, Figs. 2A-2D; Ex.1002, ¶¶139-140.

Therefore, *Kaufman* discloses that “the new password [*Jonsson* response code] is generated by concatenating [the concatenating operation that occurs prior to application of *Kaufman*'s hashing algorithm] the token [*Jonsson*'s received challenge code] and the passcode [*Jonsson*'s PIN].” Ex.1002, ¶141.

C. Ample Motivation Existed to Combine *Veneklase, Jonsson, Sormunen, and Kaufman*

First, like the other three references, a POSITA would have appreciated that *Kaufman* is analogous art that is within the same field of endeavor and addresses the same problems as that of the '658 Patent. Like the '658 Patent, *Kaufman* discloses a method “by which an authentication server in a distributed computing system may transmit an authentication ‘ticket’ to a user, authorizing access by the user to specified system resources.” Ex.1008, 1:25-28; *see* Ex.1001, 1:7-11.

Additionally, *Kaufman* addresses similar problems as the '658 Patent. The '658 Patent notes that “passwords created by users are often combinations of words and names, which are easy to remember but also easily guessed” and “guessing passwords is a frequent technique used by ‘hackers’ to break into systems.” Ex.1001, 1:28-31. Similarly, *Kaufman* explains that “[a]n

authentication system based solely on passwords and user names is open to attack by would-be intruders,” that “user names often are not difficult for unauthorized persons to determine,” and that “when users are allowed to select their own passwords, they tend to choose passwords that are easily remembered...[and] can be easily guessed as well.” Ex.1008, 2:8-15.

Like the '658 Patent, Kaufman discloses leveraging the “SecurID product” as a token generator to maintain security while enabling access to remotely stored information. *Compare* Ex.1008, 8:57-60 (“The token generators 520, 522 may, for example, comprise units such as SecurID™.”), *with* Ex.1001, 1:56-59; Ex.1002, ¶¶142-45; *see* Sections IX.B, IX.E.

Second, a POSITA would have been motivated to implement *Kaufman*’s teachings in combination with *Veneklase*, *Jonsson*, and *Sormunen* to achieve the benefits that *Kaufman* provides. For instance, *Veneklase* discusses potential drawbacks associated with “prior encryption techniques,” for example that they are “relatively costly and complicated and require one or more known ‘encryption keys’ which are in constant exchange between users” and are thus “susceptible to theft and/or inadvertent disclosure.” Ex.1005, 2:37-48. Part of *Veneklase*’s solution to this (and other) identified issue(s), is to rely on individualized passwords that are known to the user, as well as sending a randomly generated token, as discussed above at length.

Similarly, *Kaufman* includes a detailed discussion of prior encryption techniques and parts of the downfalls of these different systems. *See* Ex.1008, 1:35-44. Also like *Veneklase*, *Kaufman* utilizes known passwords and randomly generated tokens to overcome some of the issues associated with encryption techniques, as also discussed above. *Kaufman* further increases security at least by concatenating the password and token and hashing that concatenated string to compute a “transmission code.” *See* Ex.1008, 9:41-10:17.

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” (Ex.1008, 7:2-5) in order to add an additional layer of security, which is the primary problem to be solved by *Veneklase*’s system. Ex.1002, ¶¶146-48.

Third, a POSITA would be further motivated to implement *Kaufman*’s “hashing algorithm” into *Veneklase*’s system because the combination merely uses a known technique to improve similar devices in a similar way. *KSR*, 550 U.S. at 417. For example, 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 or additional process that would have been applied to generating *Veneklase*’s “random number code.” A POSITA would have also had a reasonable

expectation of success in modifying these systems by combining them. Ex.1002, ¶¶149.

Therefore, a POSITA would have been motivated to modify, and would have had a reasonable expectation of success in modifying, *Veneklase*'s authentication system with *Jonsson*'s teachings related to its algorithm, *Sormunen*'s teachings related to the use of a cellular network, and *Kaufman*'s "hashing algorithm." Ex.1002, ¶150.

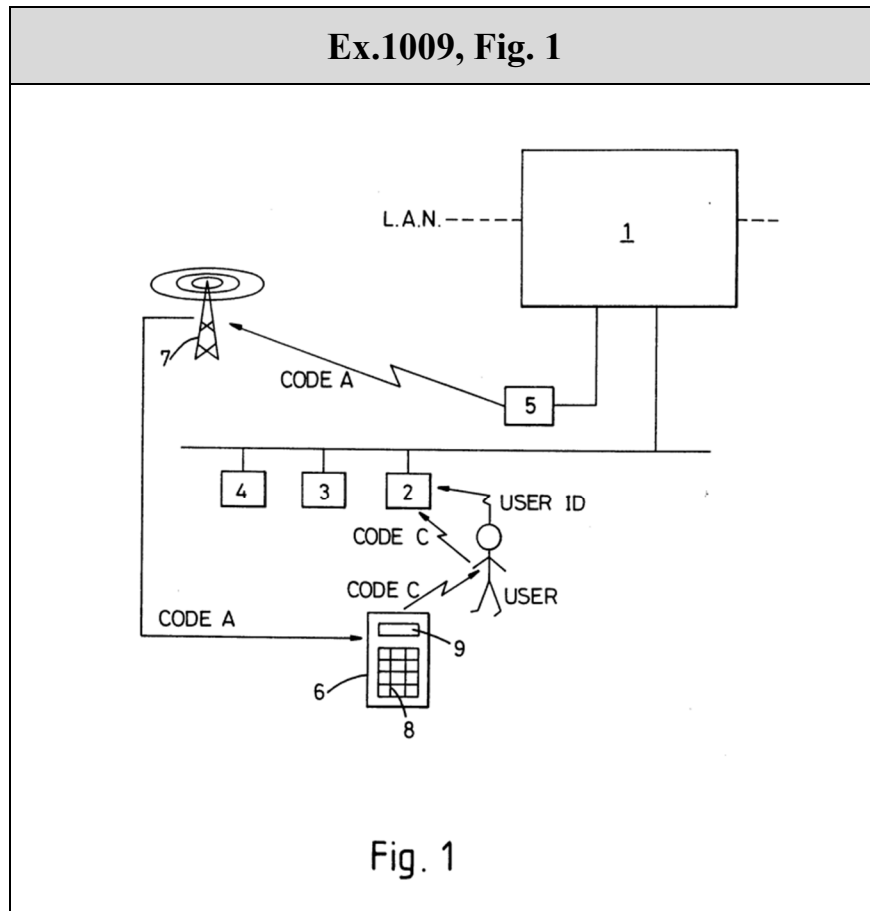
XI. GROUND #3: CLAIM 7 IS OBVIOUS OVER *KEW* IN VIEW OF *SORMUNEN*

Claim 7 depends from claim 6, and indirectly from claim 5, and the combination of *Kew* and *Sormunen* renders the limitations of claims 5-7 obvious.

A. Claim 5

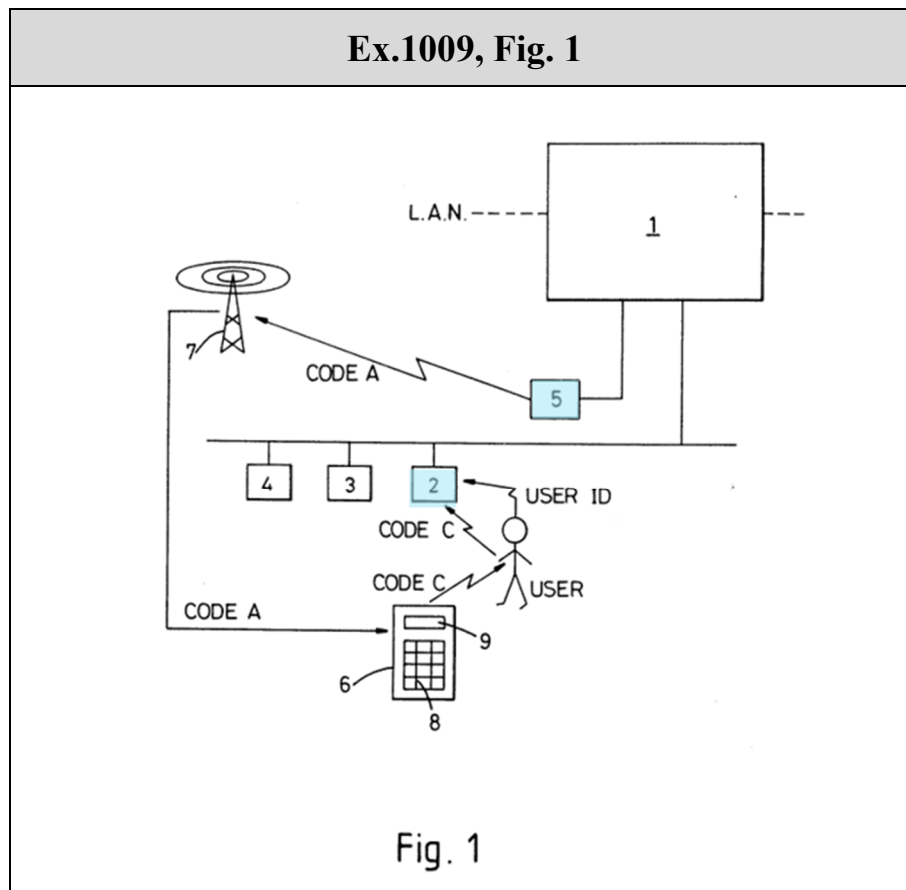
1. 5[pre]

To the extent the preamble is limiting, *Kew* discloses an authentication system. See Ex.1009, Abstract, 1:3-5, 1:20-2:23, 7:10-35, Fig. 1; Ex.1002, ¶¶151-52.



2. 5[a]

Kew discloses that computer terminal 2 operates “at the behest of the security server 5,” and “also comprises a **central processing unit (CPU)** in its own right.” Ex.1009, 9:5-11, 10:4-12, Fig. 1.



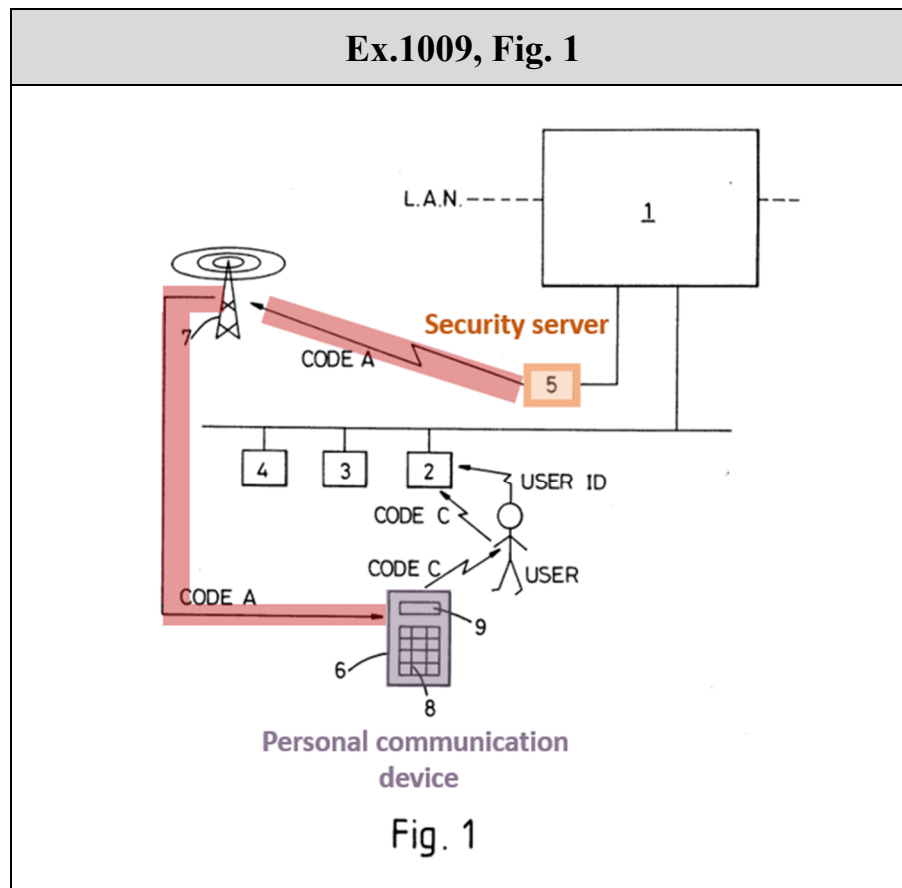
A POSITA would have understood *Kew*'s disclosure to teach that both computer terminal 2 and security server 5 contain a central processing unit. Ex.1002, ¶¶153-55.

3. 5[b]

Kew, alone or in combination with *Sormunen*, teaches or renders obvious this limitation. Ex.1002, ¶¶156-63. *Kew* discloses that “security server 5 includes a database of all authorised users and their authorised receiver units 6, and identifies the corresponding identity code for the appropriate receiver unit 6,”

which could be a personal communication device such as a pager. Ex.1009, 8:2-5, 8:12-23.

Kew additionally teaches a personal communication device configured to communicate over a cell phone network with the user authentication system. *Kew* discloses that “security server 5 also transmits...to a paging system 7,” and that transmitted information is then “broadcast by the paging system 7, typically using a radiofrequency transmitter,...similar to conventional paging systems.” Ex.1009, 8:13-19. “[T]he receiver unit 6 will use the identifier to pick out the appropriate signal.” *Id.*, 8:20-21.



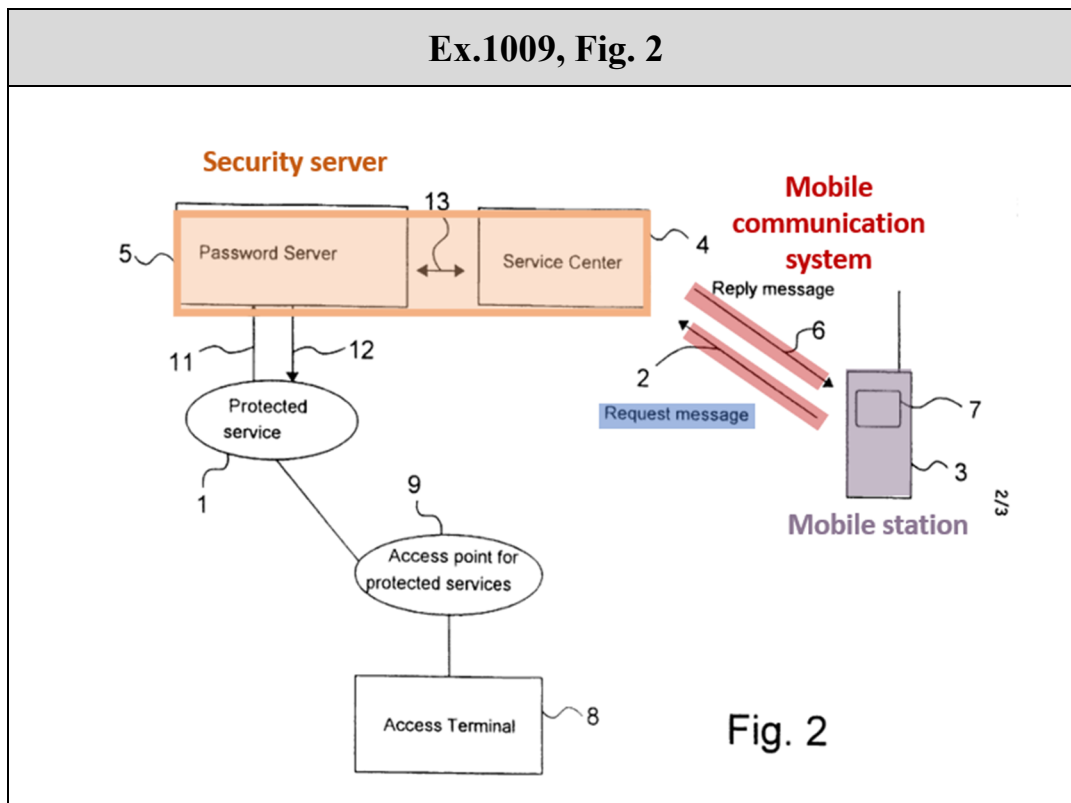
A POSITA would have understood that *Kew*'s communication channel is analogous to the networks disclosed in the '658 Patent, which include cellular and pager networks. *See* Ex.1001, 5:34-40 ("The communication module 118 forwards tokens 156 to a text messaging service provider 104, which may be a pager or mobile phone service provider."), Abstract, 1:10-11, 2:6-8, 2:28-31, 3:1-3, 4:13-17, 9:45-54; Ex.1002, ¶¶157-58.

To the extent PO asserts that *Kew*'s pager network does not disclose the claimed cell phone network, a POSITA would have found it obvious to implement the authentication system of *Kew* using a cell phone network. *KSR*, 550 U.S. at 418-19. *Kew* explicitly contemplates that the device 6 and the security server 5 communicate via "radiofrequency transmitter[s]." Ex.1009, 8:12-23. While the example provided in *Kew* is a pager system, a POSITA would have found it obvious to use a cell phone network, which is another type of communication that utilizes radiofrequency transmission. In addition, it would have been obvious to use a cell phone network to send *Kew*'s random code (Code A) because doing so would have made the system available to even more users in more locations, which is one of the intentions of the reference. *Id.*; *see* Ex.1009, 4:8-12, 8:15-23, 13:29-14:6. It would also have been obvious because cell phones are preferred to pagers for multiple reasons, such as for their larger screens, buttons, and user interfaces.

Ex.1002, ¶159. A POSITA would have had a reasonable expectation of success in modifying *Kew*'s authentication system to use a cellular network instead of a pager network because they operate similarly, many times using the same protocols, and would only involve swapping out devices and making routine software configuration changes. *Id.*

Thus, *Kew* teaches a user database configured to associate a user with a personal communication device possessed by the user (*e.g.*, a database of all authorized users and their authorized receiver units), said personal communication device (*e.g.*, receiver unit 6) configured to communicate over a cell phone network (*e.g.*, communicates over a radiofrequency transmission network) with the user authentication system (*e.g.*, security server 5). Ex.1002, ¶160.

To the extent it is argued that *Kew* does not teach or render obvious the use of a cell phone network, *Sormunen* discloses a personal communication device (*e.g.*, mobile phone) configured to communicate over a cell phone network (*e.g.*, a GSM system). *See* Ex.1007, 5:35-38, Fig. 2; Ex.1002, ¶161.



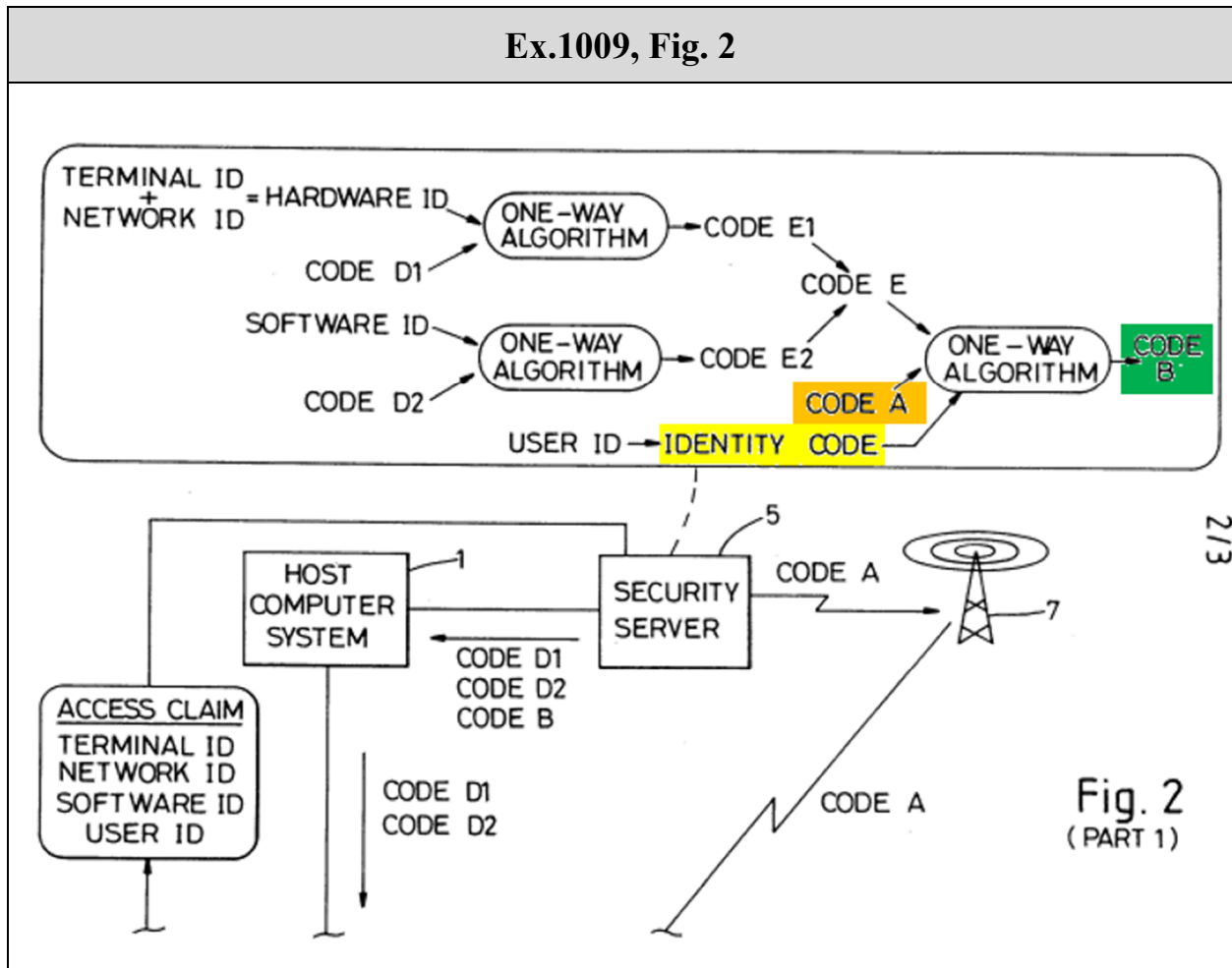
Sormunen discloses that “[t]he present invention can be applied especially in such telecommunication systems in which it is possible to transmit short messages to a terminal belonging to the telecommunication system on the basis of a terminal key, such as a telephone number” and that “[t]his quality is included in mobile communication systems,” which “include[s] for example a **cellular system**, a paging system, and a **mobile phone system**.” Ex.1007, 4:30-5:8. *Sormunen* discloses that a “**cellular system, such as the GSM system**, is a mobile communication system in which a **cellular network** is used.” *Id.*

Thus, *Kew* alone, and certainly in combination with *Sormunen*, discloses this limitation. Ex.1002, ¶¶162-63.

4. 5[c]

Kew teaches or renders obvious this limitation. Ex.1002, ¶¶164-68. *Kew* discloses that after the user enters his user identification code, “the security server 5 then **generates a random code (Code A)** and subjects this number to an encryption using the same one-way algorithm as is stored in the user’s receiver 6 together with the corresponding **identity code**” to create a “**transformed code (Code B)**.” Ex.1009, 8:5-10. *Kew* further discloses that “the security server 5 also transmits the random code [(Code A)] to a paging system 7 along with an identifier or identifying tag which can be recognized by the receiver unit 6.” *Id.*, 8:12-15.

Kew discloses that after the receiver unit 6 receives the random code (Code A), it “uses the received random number and the identity code stored in its own EPROM to produce a transformed code (Code C) via its own characteristic algorithm,” which is the same as the one used by the security server 5 to produce transformed code (Code B). *Id.*, 8:33-36. Although Figure 2 includes a more complicated embodiment utilizing additional Code E, the simpler embodiment discussed here shows how the **new password (Code B)** is created based on both the **user’s identity code** and the **randomly generated code (Code A)**. Ex.1009, Fig. 2.



Because Code A is randomly generated by security server 5, Code A is not known to the user prior to it being sent to the receiver unit. 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.

Kew additionally discloses that "terminal 2, at the behest of the security server 5 prompts the user to input the transformed Code C displayed by the receiver unit 6" and that "security server 5 [then] **compares the input Code C**

with the transformed code, Code B, it produced by encryption of the random code, Code A.” Ex.1009, 9:5-11. Therefore, a POSITA would have understood that *Kew*’s security server is setting transformed Code B—that the security server created by encryption of random Code A—to be the new password, *i.e.*, the password against which the user’s input code (Code C) is compared. Ex.1002, ¶167.

Thus, *Kew* teaches a control module executed on the computer processor (*e.g.*, a portion of security server 5) configured to create a new password (*e.g.*, transformed code (Code B)) based at least upon a token (*e.g.*, previously unknown random code (Code A)) and a passcode (*e.g.*, user’s known identity code), wherein the token is not known to the user but the passcode is, the control module further configured to set a password associated with the user to be the new password (*e.g.*, using transformed code (Code B) as the new password). Ex.1002, ¶168.

5. 5[d]

Kew teaches or renders obvious this limitation. Ex.1002, ¶169. *Kew* discloses that its system includes “transmitting Code A [the randomly generated token] via a paging system, to a receiver held by the user.” Ex.1009, 1:31-32. As discussed in Section XI.A.3, “the security server 5 also transmits the random code to a paging system 7” and “[t]he identifying tag and the random code are then broadcast by the paging system 7, typically using a radiofrequency transmitter, in a

fashion similar to conventional paging systems.” *Id.*, 8:12-19. As discussed in Section XI.A.3, *Kew*’s communication channel is akin to the cellular and pager networks disclosed in the ’658 Patent, and at the very least, a POSITA would have found it obvious to use a cellular network for the transmission of *Kew*’s randomly generated token to a personal communication device.

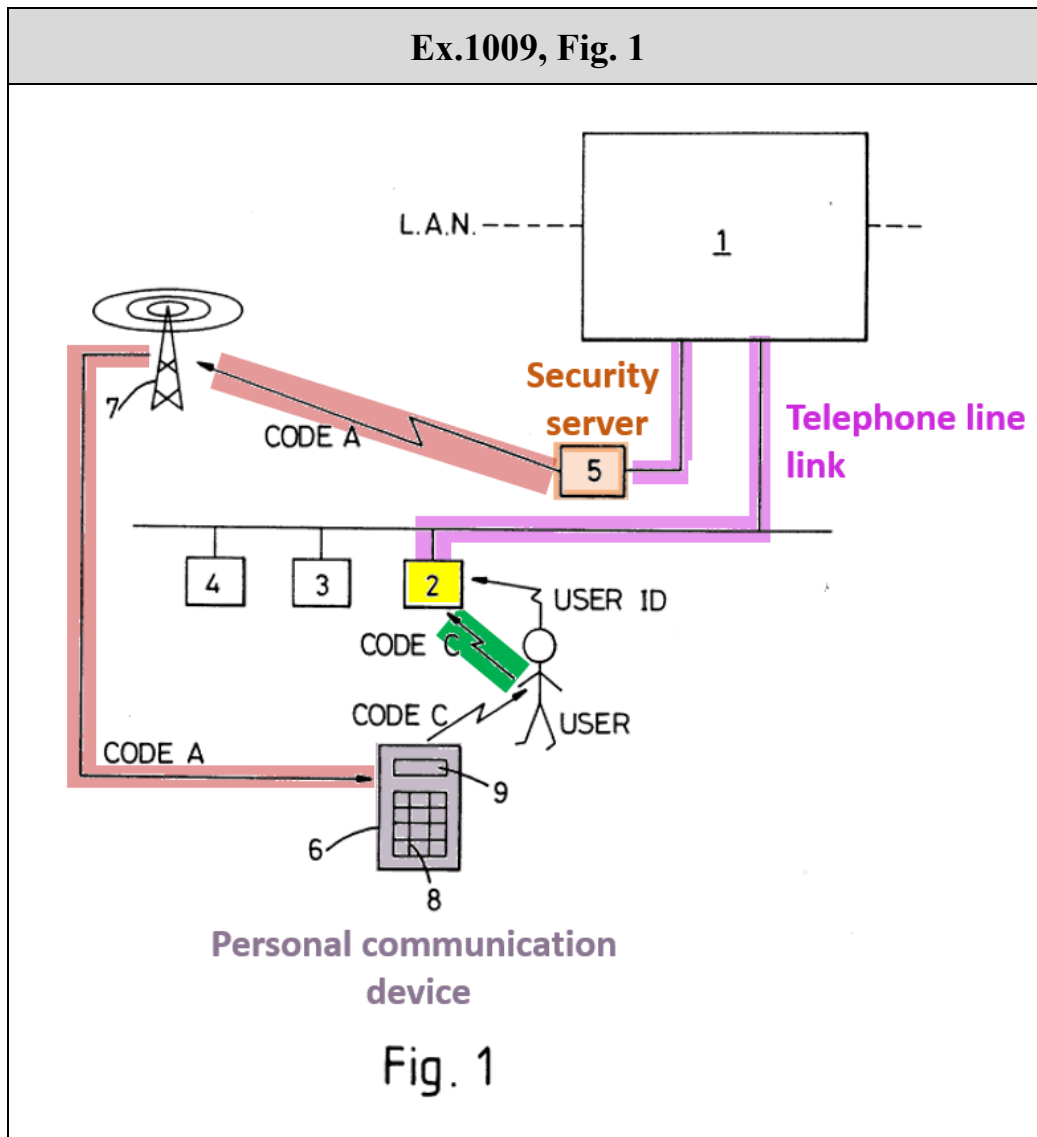
Kew (as well as *Kew* in combination with *Sormunen*) therefore teaches a communication module (*e.g.*, a portion of security server 5) configured to transmit the token to the personal communication device through the cell phone network (*e.g.*, transmit the random code (Code A) to a receiver via a paging system).

Ex.1002, ¶¶169-70.

6. 5[e]

Kew teaches or renders obvious this limitation. Ex.1002, ¶¶171-73. *Kew* discloses an authentication module (*e.g.*, a portion of security server 5) configured to receive the password from the user through a secure computer network (*e.g.*, user is prompted by server 5 to input Code C). Specifically, *Kew* discloses that “the **receiver unit 6**...uses the received random number and the identity code stored in its own EPROM to produce a transformed code (Code C),” which is “then displayed to the user.” Ex.1009, 8:33-9:3. “[T]erminal 2, at the behest of the security server 5 **prompts the user to input the transformed Code C displayed by the receiver unit 6.**” *Id.*, 9:5-7. This information is entered into a remote

terminal 2, which is connected to the host computer system 1 “via a telephone line link.” *Id.*, 7:10-14, Fig. 1.



A POSITA would have understood that this connection, which is different from the pager network connecting the system to the personal receiver device, is secure at least because the connection requires that a user verify their identity.

Ex.1002, ¶¶172-73. For example, *Kew* discloses “a computer security system...for

preventing unauthorized access to a host computer system.” Ex.1009, 1:3-5. *Kew* further discloses that “[t]o gain access to the host system 1, a user at one of the terminals, say terminal 2, must first verify his or her identity by satisfying a security barrier system or security server 5, which is effectively interposed between the remote terminals 2, 3, 4 and the host system 1.” Ex.1009, 7:10-18. This is similar to what the ’658 Patent describes, which is “for a secure system, such as a computer system.” Ex.1001, 1:63-65; *see id.*, 2:49-3:3, 4:9-26.

7. 5[f]

Kew discloses or renders obvious this limitation. Ex.1002, ¶¶174-181.

Activates Access – Unified IPR Board Construction. To the extent the Board here adopts the same construction as in the Unified IPR (Ex.1013, Paper 9 at 24), *Kew* discloses wherein the authentication module (*e.g.*, a portion of security server 5) activates access to the account in response to the password (*e.g.*, if Code B and Code C match, access to host system 1 is permitted). Specifically, *Kew* discloses that once the user has input the transformed Code C, “**the security server 5 compares the input Code C with the transformed code, Code B**” and “[i]f Code B and Code C are identical, access to the host system 1 is permitted.” Ex.1009, 9:5-11, 1:36-2:3.

Activates Access – District Court’s Construction. To the extent the Board here adopts Judge Payne’s construction (Ex.1011, p. 16), *Kew* renders obvious this

limitation. A POSITA would have recognized that when Kew's transformed code (Code B) is created, the "database of all authorised users" is updated to associate Code B with the appropriate user and devices. Ex.1009, 7:34-8:10. The POSITA would have also recognized, or at least found it obvious, that this password creation and association in the database would activate the user account such that—after the creation of Code B—it could be readily accessed by a user. For additional security, it would have further been obvious to allow for the account to be activated so that it could be accessed by inputting Code C on the personal communication device. Ex.1002, ¶¶175-76.

In addition, *Kew* discloses wherein the user has an account on the secure computer network. For example, *Kew*'s "security server 5 includes a database of all authorised users and their authorised receiver units." Ex.1009, 8:2-5. A POSITA would have understood that in order for the user to be listed in the database as an authorized user, they would need to have an account on the secure computer network. Ex.1002, ¶177.

Additionally, *Kew*'s system deactivates the account within a predetermined amount of time after activating the account (*e.g.*, enabled for a predetermined period), such that said account is not accessible through any password via the secure computer network (*e.g.*, an unauthorized user cannot gain access to the system even if he has possession of the receiver and knows the user identification

code). Specifically, *Kew* discloses that “**the receiver can only be enabled for a predetermined period to permit it to transform the received Code A to the transformed Code C by input of a second user identification code by the user.**” Ex.1009, 3:14-17. In other words, a user only has a certain “predetermined period” to input the code required for access to the system. After that predetermined period of time, “an unauthorised user **cannot gain access to the system** even if he has possession of the receiver and knows the user identification code without knowledge of the second identification or activation code.” *Id.*, 3:19-23. By only enabling the transformation of received Code A to transformed Code C, which requires the input of a user identification code, *Kew* disables a user’s access to the system after the predetermined time period.

Moreover, *Kew* further discloses that after the receiver uses the received random number and the identity code to produce the transformed Code C, the “transformed Code C is then displayed to the user on a display means 9...for a predetermined length of time such as five minutes.” Ex.1009, 8:33-9:3. By only displaying the transformed Code C that is required for system access for a predetermined period of time, *Kew* effectively deactivates the account by not allowing access to the account via any password. Ex.1002, ¶¶178-181.

Kew's teaching is nearly identical to the '658 Patent's description. *See* Ex.1001, Fig. 5, 9:61-64 ("At a step 520, upon expiration of the token 156, the control module 402 deactivates the user account in the user database 114.").

B. Claim 6

Claim 6 depends from claim 5, which is obvious in view of *Kew* and *Sormunen* as discussed above in Section XI.B incorporated herein.

Kew teaches or renders obvious this limitation. Ex.1002, ¶¶182-84. *Kew* discloses that "[w]hen the user seeks access to the host system 1 via the terminal 2, he enters his user identification code." Ex.1009, 7:34-35. Upon receiving the user identification code, "security server 5 then generates a random code (Code A) and subjects this number to an encryption using the same one-way algorithm as is stored in the user's receiver 6 together with the corresponding identity code." *Id.*, 8:5-10. In doing so, "transformed code (Code B) is produced." *Id.* Therefore, a POSITA would have understood that the user's submission of his user identification code serves as a request for the token (*e.g.*, random Code A) to be sent to their personal receiver device and the security server also creates the new password (*e.g.*, transformed Code B) in response to the request. Ex.1002, ¶¶183-84.

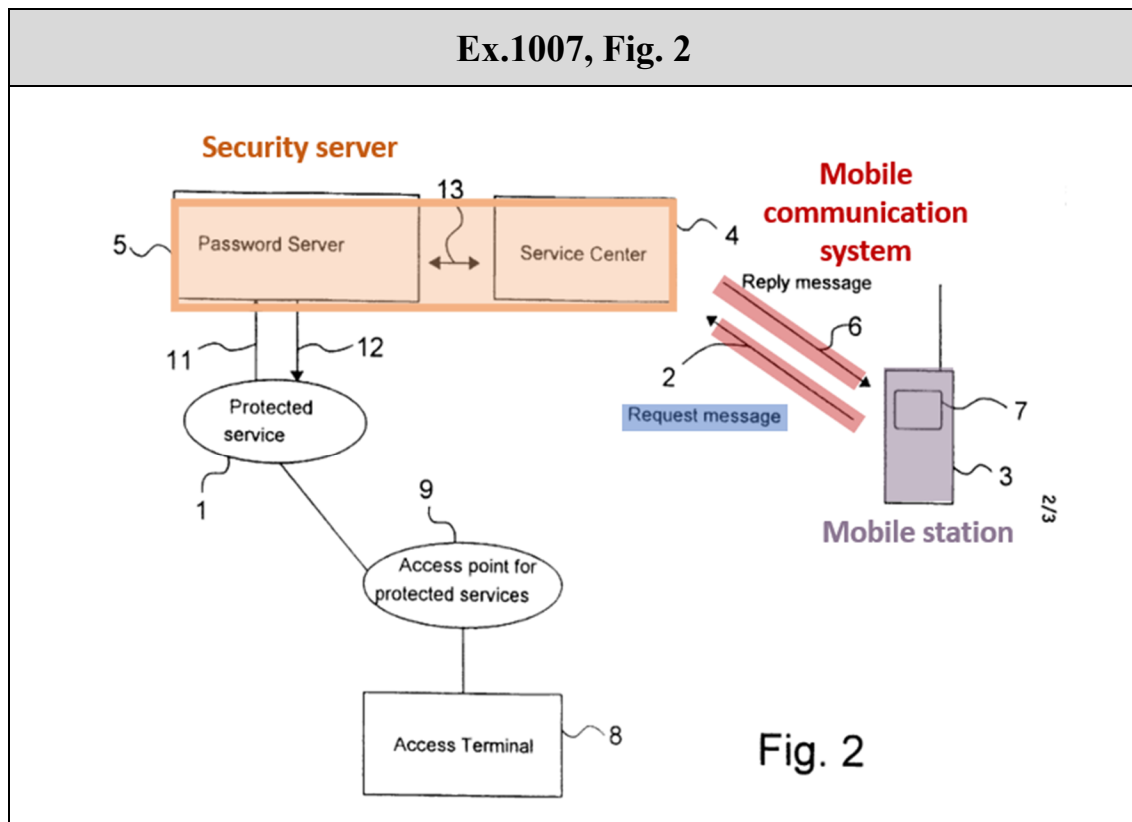
Thus, *Kew* teaches wherein the communication module is further configured to receive a request from the user for the token (*e.g.*, receives a communication that

leads to the creation of random Code A), and wherein the control module is further configured to create the new password in response to the request (*e.g.*, transformed Code B is produced in response). *Id.*

C. Claim 7

Claim 7 depends from claim 6, which is obvious in view of *Kew* and *Sormunen* as discussed above, incorporated herein. Claim 7 adds: “wherein the request is transmitted by the user through the personal communication device.”

Claim 7 is rendered obvious by *Kew* in view of *Sormunen*. Ex.1002, ¶¶185-89. Specifically, *Sormunen* discloses that in order to obtain a password or list of passwords, “the user of the service **sends a short message 2 from the paging terminal 3, such as a mobile station.**” Ex.1007, 5:35-38, Fig. 2.



Sormunen discloses that “the **short message 2 includes a password request.**” Ex.1007, 5:38-6:1. In combination with *Kew* described with respect to claim 5, a POSITA would have understood that this request would be for a token (e.g., *Kew*’s random code: Code A).

Upon receiving the password request 2, *Sormunen*’s “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.” Ex.1007, 6:20-24. *Sormunen* notes that “[t]he present invention can be applied especially in such telecommunication systems in which it is possible to

transmit short messages...on the basis of a terminal key, such as a telephone number” and that “[t]his quality is included in mobile communication systems,” such as “a **cellular system, a paging system, and a mobile phone system.**” *Id.*, 4:30-5:8.

D. Ample Motivation Existed to Combine *Kew* and *Sormunen*

It would have been obvious to incorporate *Sormunen*’s teachings related to an authentication system in which a mobile phone communicates with the authentication system to request a token via a cellular network with *Kew*’s authentication system that utilizes conventional paging systems to communicate between a receiver unit and a security server. Ex.1002, ¶¶190-96.

First, *Kew* and *Sormunen* are analogous art because they are in the same field of endeavor as the ’658 Patent. *Compare* Ex.1001, 1:7-11 (’658 Patent “relates generally to the authentication of user[s] of secure systems”) *with* Ex.1009, Abstract (“method of preventing unauthorised access to a host computer system...Code A is transmitted via a paging system (7), to a receiver (6) held by the user”), *and* Ex.1007, Abstract (“method for obtaining at least one item of user specific data...at least partly by using paging or a short message service”). In addition, both references are reasonably pertinent to another aspect of the ’658 Patent, namely, authenticating user access using a mobile phone or pager. Ex.1001, 1:56-59. *Kew* solves the same problem by using a generated random

code sent to a personal communication device. *See* Ex.1009, 8:15-19. Similarly, *Sormunen* sends authentication information via a mobile network. *See* Ex.1007, 4:30-5:8; Ex.1002, ¶191.

Second, a POSITA would have been motivated to combine *Kew* with *Sormunen* in order to broaden access to the invention disclosed in *Kew* and access the benefits disclosed in *Sormunen*. *Kew* teaches a system in which a random code can be sent from a security server to a receiver unit via “conventional paging systems.” *See* Ex.1009, 8:12-23. *Sormunen* discloses a similar authentication system that allows a paging device to communicate with the authentication system via a cellular network, such as the well-known GSM system. *See* Ex.1007, 4:30-5:8. A POSITA would have been motivated to make such a combination because it would have allowed *Kew*’s authentication system to operate on the well-known and ubiquitous GSM system. Ex.1002, ¶192.

Furthermore, a POSITA would have been motivated to make such a combination because implementing *Kew*’s authentication system on *Sormunen*’s cellular network would allow for two-way communication between the receiver unit and the security server, and thus allow the user to request a random code via the receiver unit, as well as the terminal, which is precisely what is disclosed in *Sormunen*. Ex.1007, 7:34-35. Indeed, a POSITA would recognize that by implementing *Kew*’s authentication system on the widely available GSM system

disclosed in *Sormunen*, *Kew*'s system would obtain *Sormunen*'s benefits of allowing for secure access to a service "almost immediately" after a request is sent. Ex.1007, 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"); Ex.1002, ¶193.

A POSITA would have also recognized that adding *Sormunen*'s functionality for a user to remotely request a token, for example through *Sormunen*'s mobile device, would, in addition to broadening access to the system in *Kew*, increase efficiency and add desired features to *Kew*'s system. For instance, if a user attempts to access the system disclosed in *Kew* but is unable to locate the token or the token expires, the user would have to initiate the initial request through the remote terminal once again. By modifying the system in *Kew* with *Sormunen*, the user would be able to directly request the token from a mobile device already in their hands. This would improve user-friendliness of the system and provide desirable and marketable features without compromising security. The combined system of *Kew* and *Sormunen* would implement *Kew*'s database to confirm that a token request came from the appropriate user. See Ex.1009, 8:2-5. A POSITA would have recognized that this 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. Ex.1002, ¶194.

Third, *Kew* explicitly provides a teaching, suggestion, and motivation for combining it with an authentication system that operates on other types of networks, such as those taught in *Sormunen*, because it explicitly discloses the use of a radiofrequency transmitter, which is also used in other systems, such as the GSM network. *See* Ex.1009, 8:15-19. Thus, a POSITA would have been motivated to use *Kew*'s authentication system in conjunction with receiver units that can operate on a cellular network, such as that described in *Sormunen*, to provide additional flexibility and features. Ex.1002, ¶195.

Fourth, a POSITA would have further been motivated to combine *Kew* and *Sormunen* and had a reasonable expectation of success because the combination uses a known technique to improve similar devices in the same way. For example, a POSITA would have been motivated to utilize the cellular network functionality of *Sormunen* in *Kew*'s system because it would have been used in the same way—*e.g.*, to allow communication between a mobile device unit and a central server. *Kew* discloses the use of radiofrequency transmitters operating via conventional systems (*e.g.*, paging systems), so it would have been obvious for a POSITA to combine it with *Sormunen*, which teaches that such a system can operate on paging

systems as well as cellular systems and mobile systems. *See* Ex.1007, 4:30-5:9; Ex.1002, ¶196.

XII. GROUND #4: CLAIM 2 IS OBVIOUS OVER *KEW* IN VIEW OF *SORMUNEN* AND *KAUFMAN*

Claim 2 depends from claim 1, which is rendered obvious by *Kew* in view of *Sormunen*. Ex.1002, ¶¶197-205.

A. Claim 1

As shown in the chart below, and with the exception of limitation 1[b], claim 1 recites limitations analogous in scope to those of claim 5. The corresponding sections referenced in the chart below are incorporated by reference herein.

Claim 1 Limitation	Corresponding Analogous Claim 5 Limitation(s)	Section(s) Incorporated By Reference
1[pre]	5[pre], 5[e], 5[f]	XI.A.1, XI.A.6, XI.A.7
1[a]	5[b], 5[e]	XI.A.3, XI.A.6
1[b]	<i>See</i> Claim 7 and below	<i>See</i> XI.D
1[c]	5[c]	XI.A.4
1[d]	5[c]	XI.A.4
1[e] ¹¹	5[f]	XI.A.7
1[f]	5[d]	XI.A.5
1[g]	5[e]	XI.A.6
1[h]	5[f]	XI.A.7

¹¹ This limitation is rendered obvious as discussed with respect to the section titled “Unified IPR Board Construction” in Section XI.A.7.

1. 1[b]—“receiving a request from the user for a token via the personal communication device, over the second network;”

Kew in combination with *Sormunen* renders obvious this limitation.

Ex.1002, ¶¶199-201; *see supra* Section XI.A.C (claim 7). As also discussed with respect to Ground 2’s discussion of limitation 1[b] (Section X.A.1, incorporated here), *Sorumunen* discloses the elements of claim 1[b]. In the combination with *Kew* described with respect to claim 5, a POSITA would have understood that *Sormunen*’s “short message 2 [that] includes a **password request**” (Ex.1007, 5:35-6:1, Fig. 2) would be a request for a token (e.g., random code (Code A)).

Thus, *Kew* in combination with *Sormunen* discloses wherein the request (e.g., a password request) is transmitted by the user through the personal communication device (e.g., receiver unit/paging terminal) over the second network (e.g., cellular network). Ex.1002, ¶201.

B. Claim 2

Claim 2 adds “wherein the new password is generated by concatenating the token and the passcode.” *Kew* in combination with *Sormunen* and *Kaufman* renders obvious this limitation. Ex.1002, ¶¶202-205.

As discussed previously, *Kaufman* discloses a system utilizing a password and a token, and that “workstation 516 **computes a ‘transmission code’ based upon the password and the token**” and that “the transmission code is calculated

by using a first ‘hashing algorithm.’” Ex.1008, 9:40-43. *Kaufman*’s “hashing algorithm” is “a one-way routine for transmuting multiple input data items, [that] **concatenate[es] selected items of the input data** and perform[s] a ‘hashing equation’ upon one or more items of the input data, in a specified order.” *Id.*, 9:43-46. The disclosed “hashing equation” can include “any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence.” *Id.*, 9:47-53; Ex.1002, ¶203.

Kaufman discloses different hashing algorithms that may be used to concatenate tokens and passcodes:

[H]ashing algorithm 1.0, explained more fully, comprises the following operations: the password is modified by the selected hashing equation, the **modified password is concatenated onto the token to form a concatenation**, and this concatenation is modified by the hashing equation. The system may be designed so that a specified single hashing algorithm, such as one of the algorithms 1.0-1.3, is used at all times; alternatively, a number of variations are contemplated, such as the use of a selected algorithm during specified time periods by specified workstations.

Ex.1008, 10:7-17. *Kaufman* explains that, in connection with the table presented in the specification, reproduced below, that “the ‘|’ symbol represents the

concatenation operation.” *Id.*, 10:6-7.

Ex.1008, Hashing Algorithms Disclosed in <i>Kaufman</i>	
[1.0]	hash(token hash(password))
[1.1]	hash(hash(password token)
[1.2]	hash(token password)
[1.3]	hash(password token)

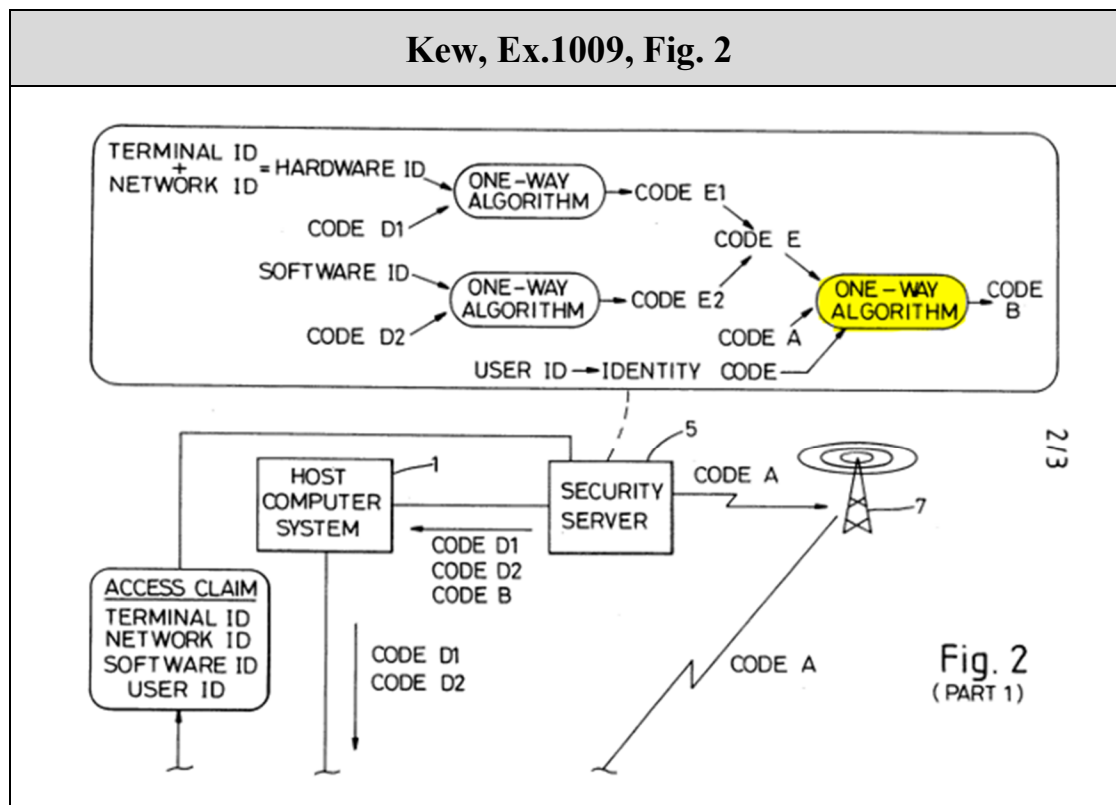
Id., 9:65-10:5. A POSITA would appreciate that *Kaufman* discloses the generation of a password (Kaufman’s “transmission code”) through concatenation of a token and password. A POSITA would also appreciate that *Kaufman*’s system is the same as the one claimed in the ’658 Patent. *See* Ex.1001, 4:52-53, Figs. 2A-2D; Ex.1002, ¶¶203-04.

Thus, *Kew* in combination with *Sormunen* and *Kaufman* discloses wherein the new password (e.g., transmission code) is generated by concatenating the token and the passcode. Ex.1002, ¶205.

C. Ample Motivation Existed to Combine *Kew*, *Sormunen*, and *Kaufman*

First, as previously discussed in Section X.C., a POSITA would have appreciated that *Kaufman* is within the same field of endeavor and is reasonably pertinent to a problem addressed in the ’658 Patent. Ex.1002, ¶¶206-13; Section X.C.

Second, a POSITA would have been motivated to combine the teachings of *Kaufman* with *Kew* and *Sormunen*'s teachings because the combination would have been an obvious result applying a known technique in another system to obtain improved and predictable improvements in security. *Kew* discloses that its system can be utilized in connection with encryption techniques and repeatedly discusses that its system utilizes transformation and one-way algorithms to generate various codes. *See* Ex.1009, 7:34-8:10 (random Code A “encrypt[ed] using the same **one-way algorithm**...together with the corresponding identity code. In this way a transformed code (Code B) is produced.”), 7:20-32 (describing use of “**one-way algorithm**”); *see id.*, 11:20-12:5, 12:19-34, Fig. 2.



Kew, however, does not disclose details of what particular algorithm is utilized and explains that “transformation algorithms associated with each receiver may be completely different.” Ex.1009 at 3:1-6.

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. Ex.1008, 9:41-10:17 (describing a “hashing algorithm” as “a **one-way routine**...[that] concatenat[es] selected items of the input data and perform[s] a ‘hashing equation’ upon one or more items of the input data, in a specified order”).

Ex.1008, Hashing Algorithms Disclosed in <i>Kaufman</i>	
[1.0]	hash(token hash(password))
[1.1]	hash(hash(password token)
[1.2]	hash(token password)
[1.3]	hash(password token)

This is especially true with respect to *Kaufman*’s disclosed algorithms that are similarly focused on increasing security in systems that can be used in connection with encryption techniques. See Ex.1008, 7:2-5 (“cryptographically secure hashing algorithm”), Abstract; Ex.1002, ¶¶207-11.

Third, because *Kew*'s system calls for a one-way algorithm for improving security and *Kaufman* discloses such a one-way algorithm through the use of, for example, concatenation and hashing to achieve security and deter hacking, a POSITA would have had a reasonable expectation of success in modifying *Kew* in view of *Sormunen* and *Kaufman*. Ex.1002, ¶¶212-13.

XIII. NO SECONDARY CONSIDERATIONS SUPPORT NON-OBVIOUSNESS

There is no indication that any secondary considerations exist.

XIV. CONCLUSION

Trial should be instituted to cancel the Challenged Claims.

Dated: December 18, 2023

Respectfully submitted,

/s/ Alexander B. Stein

Alexander B. Stein

Reg. No. 71,397

U.S. PATENT NO. 6,993,658 – Listing of Challenged Claims

Claim No.	Claim Limitations
1[preamble]	A method of authenticating a user on a first secure computer network, the user having a user account on said first secure computer network, the method comprising:
1[a]	associating the user with a personal communication device possessed by the user, said personal communication device in communication over a second network, wherein said second network is a cell phone network different from the first secure computer network;
1[b]	receiving a request from the user for a token via the personal communication device, over the second network;
1[c]	generating a new password for said first secure computer network based at least upon the token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user;
1[d]	setting a password associated with the user to be the new password;
1[e]	activating access the user account on the first secure network;
1[f]	transmitting the token to the personal communication device;
1[g]	receiving the password from the user via the first secure computer network; and
1[h]	deactivating access to the user account on the first secure computer network within a predetermined amount of time after said activating, such that said user account is not accessible through any password, via said first secure computer network.
2	The method of claim 1, wherein the new password is generated by concatenating the token and the passcode.
5[preamble]	A user authentication system comprising:
5[a]	a computer processor;
5[b]	a user database configured to associate a user with a personal communication device possessed by the user, said personal

Claim No.	Claim Limitations
	communication device configured to communicate over a cell phone network with the user authentication system;
5[c]	a control module executed on the computer processor configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a password associated with the user to be the new password;
5[d]	a communication module configured to transmit the token to the personal communication device through the cell phone network; and
5[e]	an authentication module configured to receive the password from the user through a secure computer network, said secure computer network being different from the cell phone network,
5[f]	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.
6	The system of claim 5, wherein the communication module is further configured to receive a request from the user for the token, and wherein the control module is further configured to create the new password in response to the request.
7	The system of claim 6, wherein the request is transmitted by the user through the personal communication device.

CERTIFICATION OF COMPLIANCE WITH TYPE-VOLUME LIMITS

This Petition includes 13,991 words, as counted by Microsoft Word, and is therefore in compliance with the 14,000-word limit established by 37 C.F.R. 42.24(a)(1)(i). Accordingly, pursuant to 37 C.F.R. 42.24(d), lead counsel for Petitioner hereby certifies that this Petition complies with the applicable type-volume limits.

Dated: December 18, 2023

Respectfully submitted,

/s/ Alexander B. Stein

Alexander B. Stein

Reg. No. 71,397

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b), I certify that I caused to be served a true and correct copy of the foregoing: Power of Attorney, Petition for *Inter Partes* Review of U.S. Patent No. 8,840,635 and the exhibits cited therein by Priority Express Mail on this day, December 18, 2023, on Dynapass IP Holdings LLC's correspondence address of record for the subject patent as follows:

151075 - DynaPass Inc
PO Box 11510
Costa Mesa, CA 92627
United States

A courtesy copy of this Petition and supporting exhibits was also served via email on December 18, 2023 on Dynapass IP Holdings LLC's counsel of record in the district court litigation involving this patent:

John Wittenzellner
johnw@wsltrial.com

Michael James Fagan, Jr.
mfagan@wsltrial.com

Fred Irvin Williams
fwilliams@wsltrial.com

Dated: December 18, 2023

Respectfully submitted,

/s/ Alexander B. Stein

Alexander B. Stein
Reg. No. 71,397