

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, LLC, and JPMORGAN CHASE BANK, N.A.¹

Petitioner,

v.

DYNAPASS IP HOLDINGS, LLC

Patent Owner.

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

Patent No. 6,993,658

PATENT OWNER'S REFILED SUR-REPLY TO PETITIONER'S REPLY

Filed on behalf of Patent Owner by:

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

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

WILLIAMS SIMONS & LANDIS PLLC

¹JPMorgan Chase Bank N.A. was joined as a party to this proceeding via Motion for Joinder in IPR2023-01331.

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	CLAIM CONSTRUCTION	1
III.	GROUND 1 — <i>VENEKLASE</i> AND <i>JONSSON</i> DO NOT RENDER OBVIOUS INDEPENDENT CLAIM 5.....	1
A.	The Combination of <i>Veneklase</i> and <i>Jonsson</i> Does Not Teach or Suggest Claim Element [5.3].	2
B.	The Combination of <i>Veneklase</i> and <i>Jonsson</i> Does Not Teach or Suggest Claim Element [5.4].	6
C.	The Combination of <i>Veneklase</i> and <i>Jonsson</i> Does Not Teach or Suggest Claim Element [5.5].	8
D.	The Combination of <i>Veneklase</i> and <i>Jonsson</i> Does Not Teach or Suggest Claim Element [5.6].	10
IV.	GROUND 2 — <i>KEW</i> AND <i>SORMUNEN</i> DO NOT RENDER OBVIOUS INDEPENDENT CLAIMS 1 and 5.....	13
A.	The Combination of <i>Kew</i> and <i>Sormunen</i> Does Not Teach or Suggest Claim Element [5.3].	13
1.	<i>Kew</i> ’s “identity code” is not the claimed “passcode.”	14
2.	<i>Kew</i> ’s “user identification code” is not the claimed “passcode.”	16

3.	<i>Kew</i> ’s “user identification code” and <i>Kew</i> ’s “identity code” are different.	17
B.	The Combination of <i>Kew</i> and <i>Sormunen</i> Does Not Teach or Suggest Claim Element [5.6].	19
C.	The Combination of <i>Kew</i> and <i>Sormunen</i> Does Not Teach or Suggest Claim Element [1.2].	24
V.	CONCLUSION.....	25

TABLE OF AUTHORITIES

Cases

Phillips v. AWH Corp.,

415 F.3d 1303 (Fed. Cir. 2005) (en banc).....11

Xerox Corp., et al. v. Bytemark, Inc.,

IPR2022-00624, Paper 9 (P.T.A.B. Aug. 24, 2022) (Precedential).....15

EXHIBIT LIST

Exhibit	Description
2001	Google Patents webpage for U.S. Patent No. 6,993,658, https://patents.google.com/patent/US6993658B1/
2002	“Preliminary Constructions,” <i>Dynapass IP Holdings, LLC v. JPMorgan Chase & Co., et al.</i> , No. 2:22-cv-00212-JRG-RSP (E.D. Tex.)
2003	Declaration of Rajeev Surati
2004	CV of Rajeev Surati
2005	Microsoft Computer Dictionary (5th ed. 2002)
2006	Claim Construction Order, <i>Dynapass Holdings LLC v. JPMorgan Chase & Co., et al.</i> , Case No. 2:22-cv-00212-JRG-RSP, Dkt. 120 (E.D. Tex. Oct. 31, 2023).
2007	[Expunged]
2008	Email from Board authorizing withdrawal of Ex. 2007 and refiling of Patent Owner’s Sur-Reply.

I. INTRODUCTION

Dynapass IP Holdings, LLC (“Patent Owner”) respectfully submits this Sur-Reply to Petitioner’s Reply (“Reply”) in *Inter Partes* Review No. IPR2023-00425 of U.S. Patent No. 6,993,658 (the “’658 Patent”).

II. CLAIM CONSTRUCTION

According to Petitioner, “PO’s proposed construction improperly attempts to import limitations from the specification into the claims, and should be rejected.” Reply, p. 1. Patent Owner disagrees. In fact, in its Claim Construction Order dated Oct. 31, 2023 (i.e., after the deadline for filing Patent Owner’s Response), the United States District Court for the Eastern District of Texas agreed with Patent Owner’s construction:

For the foregoing reasons, the Court construes “activates access to the account in response to the password” as “activates access to the account in response to the creation of the password.”

Ex. 2006, p. 13. The Board should adopt the same claim construction as the court.

III. GROUND 1 — *VENEKLASE* AND *JONSSON* DO NOT RENDER OBVIOUS INDEPENDENT CLAIM 5.

Petitioner misrepresents that “the Response fails to identify or consider the level of skill in the art.” Paper 16, p. 2. In fact, Patent Owner has applied Petitioner’s definition of a POSITA throughout these proceedings. *See* Paper 8, p. 11.

A. The Combination of *Veneklase* and *Jonsson* Does Not Teach or Suggest Claim Element [5.3].

Patent Owner's Response ("Response") presented two distinct rebuttals to obviousness: (1) Petitioner's proposed combination renders *Veneklase* inoperable for its intended purpose, and (2) Petitioner's proposed combination changes *Veneklase*'s principle of operation. *See* Response at 18-19. Petitioner's Reply argues that the "proffered combination would not render Veneklase's system inoperable, nor has PO demonstrated such inoperability. PO does not offer any evidence that the proposed modified system . . . would not work for Veneklase's stated goal to 'ensure that only authorized users gain access to a computer system.'" Reply, p. 3 (quoting Ex. 1005, 3:31-33) (emphasis added). As an initial matter, Patent Owner plainly did offer evidence via an expert declaration. *See* Ex. 2003, ¶¶75-79. That declaration stands unrebutted because Petitioner did not depose the expert. Further, Petitioner fails to rebut Patent Owner's showing that the proposed modification changes *Veneklase*'s principle of operation and thus is not obvious. *See* Reply, pp. 2-5.

As characterized by Petitioner, "*Veneklase* teaches a system which a user inputs a password known beforehand, receives a randomly generated previously-unknown code, and then inputs that [randomly generated code] for authentication purposes." Pet. at 31 (citing Ex. 1005, 7:52-8:27) (emphasis added). In other words,

“*Veneklase’s* system allows for authentication through user input of a known and unknown code at separate times in a two-step process.” *Id.* (emphasis added). A POSITA would understand that *Veneklase’s* principle of operation necessarily includes that two-step authentication process. *See* Response, pp. 18-19 (citing Ex. 2003, ¶76). It is undisputed that Petitioner’s proposed modification abolishes that two-step authentication process. *See* Pet., pp. 28, 31, 34; *see also* Reply, p. 4 (“Put simply, the proposed modification alters [*Veneklase’s*] method of operation . . .”); Ex. 1024, ¶5 (“the modification necessarily changes how *Veneklase* would operate”). Accordingly, Petitioner and Petitioner’s Expert concede that the proposed modification changes *Veneklase’s* principle of operation and is thus too drastic to be obvious.

Next, Petitioner argues that “the combination offers several other advantages that further *Veneklase’s* goal for secure access, such as avoiding SIM swapping and streamlining the process through only having to enter the passcode once. PO admits that requiring entry of the passcode once provides enhanced security over entering the passcode multiple times.” Reply, p. 3 (internal citations omitted) (emphasis added). That argument is misleading as shown below.

First, Patent Owner’s Response demonstrated why SIM swapping also would not work in *Veneklase’s* existing system. *See* Response, p. 21. In Reply, Petitioner offered no rebuttal to that showing. *See* Reply, pp. 2-5.

Second, Petitioner admits that *Veneklase's* “password” (the Petitioner-identified “passcode”) is already only entered once in *Veneklase's* system. *See* Pet., p. 31 (“*Veneklase* teaches a system which a user inputs a password known beforehand, receives a randomly generated previously-unknown code, and then inputs that for authentication purposes.”) (emphasis added). Specifically, *Veneklase's* “password” (the Petitioner-identified “passcode”) is only entered during the first step of the two-step authentication process. *See id.* Thus, the advantages allegedly resulting from the combination of *Veneklase* and *Jonsson* are already present in *Veneklase's* system. Accordingly, there is no motivation to combine *Veneklase* and *Jonsson*.

Petitioner argues that like *Veneklase*, the proposed “combination would still alert the user that someone is attempting to access the account” because the user would “receiv[e] a challenge code without requesting one” and thus there is no decrease in security. Reply, pp. 3-4 (citing Ex. 1024, ¶6). But neither Petitioner nor its expert cited any such evidence. *See id.* Additionally, Petitioner conveniently glosses over the fact that in *Veneklase's* system, the notification feature (i.e., generation and transmission of random code) is triggered only by receipt and successful cross-referencing of *Veneklase's* password. *See* Response, p. 20 (citing Ex. 1005, 8:2-5). That trigger sequence is part of *Veneklase's* multi-layer/level security. *See* Ex. 2003, ¶¶77-78. In contrast, the “challenge code” in the proposed

combination is generated and transmitted without needing a password. *See* Ex. 1006, 9:1-8. Accordingly, the proposed combination still dismantles *Veneklase's* multi-layer/level security, and Petitioner provides no evidence that the security of the proposed combination is superior to *Veneklase's* multi-layer/level security, so the proposed combination cannot be obvious.

Petitioner argues that “the combined system would not be ‘more prone’ to DoS attack at least because a DoS attack is not dependent on knowing a password. As such, like Jonsson and the ’658 Patent, Veneklase is susceptible to repeated requests for access from a DoS attack.” Reply, p. 5. And that “PO does not explain or offer any evidence to support this assertion other than the parroting of its expert.” Reply, p. 4. Patent Owner disagrees.

First, because Petitioner did not depose Patent Owner’s expert, his declaration stands unrebutted. *See* Ex. 1003, ¶¶79, 90. Further, as discussed in the Response, the proposed combination still requires the legitimate user to transmit an “authentication request” to the system to trigger generation and transmission of a “challenge code” to the legitimate user’s “personal communication device” (e.g., pager). Response, p. 27 (citing Ex. 1006, 9:1-4, 10:18-20, Fig. 3; Ex. 2003, ¶89). In Petitioner’s proposed combination, the “authentication request” is not a password (i.e., not a secret). Response, pp. 27-28 (citing Ex. 2003, ¶90). Accordingly, nothing prevents a hacker from continuously transmitting the non-secret “authentication

request” to the system, triggering generation and transmission of “challenge codes” to the legitimate user’s “personal communication unit” (e.g., pager)—thus interfering with the legitimate user’s access to the system. That is a denial of service (DoS) attack. *See* Ex. 1019, 1:14-16 (“A [DoS] attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.”). In contrast, *Veneklase*’s existing system requires a password (i.e., a secret) to trigger generation and transmission of the “random number code” to the legitimate user’s “pager 420.” *See* Ex. 1005, 8:1-15. Accordingly, the aforementioned DoS attack is less likely with *Veneklase*’s system because of the required password. *See* Ex. 2003, ¶90.

For these and all the reasons discussed in Patent Owner’s Response, the cited references fail to teach or suggest claim element [5.3].

B. The Combination of *Veneklase* and *Jonsson* Does Not Teach or Suggest Claim Element [5.4].

Patent Owner’s Response argued that the authentication process in the proposed combination still has two steps: (1) the user transmits *Jonsson*’s “authentication request” to the system to trigger generation of a “challenge code,” and then (2) the user transmits the “response code” to the system. *See* Response, p. 27 (citing Ex. 2003, ¶89). Thus, Petitioner’s rationale for combining *Veneklase* and *Jonsson* (i.e., “reducing the steps to a single step and thus reducing the amount of

time required,” Pet., p. 31) is not actually realized and a POSITA would not be motivated to execute the proposed combination. See Response, p. 27 (citing Ex. 2003, ¶89).

Petitioner’s Reply provides no rebuttal to that argument. See Reply, pp. 5-6. Instead, Petitioner argues “the Petition is clear that it is Jonsson’s use of only a *single transmitted password* that allows for enhanced security over the twice transmitted password of Veneklase.” Reply, p. 5 (citing Pet., pp. 30-32) (emphasis added). But by Petitioner’s own admission, *Veneklase*’s “password” is only transmitted once in *Veneklase*. See Pet., p. 31 (“*Veneklase* teaches a system which a user inputs a password known beforehand, receives a randomly generated previously-unknown code, and then inputs [the randomly generated code] for authentication purposes.”) (emphasis added). Specifically, *Veneklase*’s “password” is only transmitted during the first step of the two-step authentication process. See *id.* There is no second transmission. See *id.* Accordingly, the “enhanced security” promoted by Petitioner does not exist and thus is not a motivation to combine.

Petitioner’s arguments regarding DoS attacks are addressed above in reference to claim element [5.3]. See Reply, p. 6.

For the these and all the reasons discussed in Patent Owner’s Response, the cited references fail to teach or suggest claim element [5.4].

C. The Combination of *Veneklase* and *Jonsson* Does Not Teach or Suggest Claim Element [5.5].

In the Reply, Petitioner argues “PO alleges that *Veneklase*’s disclosure of an off-the-shelf pager requires that the pager is not capable of executing an algorithm. Response, 31. However, PO offers no evidence to support this assertion other than the nearly verbatim restatement of its expert.” Reply, p.6. That misrepresents Patent Owner’s arguments. Patent Owner actually argued “the evidence indicates that *Veneklase*’s ‘pager 420’ is not capable of executing such an algorithm.” Response, p. 31 (emphasis added). The phrase “such an algorithm” does not mean just any algorithm, but rather the “specialized security algorithms” of *Jonsson*. See Response, p. 30. Because Petitioner did not depose Patent Owner’s expert, his declaration stands unrebutted. See Ex. 2003, ¶¶95-96.

Petitioner’s Reply argues that “a POSITA would have understood from the express teachings of *Jonsson* that conventional pagers are capable of running software to execute algorithms, such as *Jonsson*’s.” Reply, p. 7 (citing Ex. 1024, ¶13). But neither Petitioner nor its expert muster any evidence that an off-the-shelf pager, in 1996, could execute *Jonsson*’s specialized security algorithms. The spectrum of computing resources necessary to execute an algorithm is vast: computing $x+1$ is an algorithm, but so are the neural networks used for artificial intelligence. So the capability for an off-the-shelf pager to execute some algorithm

(e.g., $x+1$) does not support Petitioner's argument. To the contrary, *Jonsson* itself notes that the off-the-shelf pager would still need to be customized by installing *Jonsson*'s specialized security algorithms onto the pager. See Ex. 2003, ¶96; Ex. 1006, 7:25-26 ("need to customize a communication device."). Even with his supplemental declaration, Petitioner's expert does not introduce any additional evidence to support Petitioner's argument—he merely asserts that the off-the-shelf pager in *Veneklase* can execute some non-specified algorithm. See Ex. 1024, ¶13. At bottom, Petitioner provides no evidence that a user could simply acquire an off-the-shelf pager, in 1996, and immediately start using *Jonsson*'s system without heavy hardware and/or software customization.

In contrast, *Veneklase*'s "pager 420" only needs to be capable of receiving a message and displaying the message to be ready for use in *Veneklase*'s system. See Ex. 1005, 8:1-26. But those simple algorithms are intrinsic functions (i.e., receive and display a message) of an off-the-shelf pager. That is why *Veneklase* describes "pager 420" as being a "conventional and commercially available" pager. Ex. 1005, 8:11-12. That is also why *Veneklase* describes its system as being "very cost effective." Ex. 1005, 7:21-24. Accordingly, *Veneklase* teaches away from the substantial software and/or hardware pager customization required by *Jonsson*, and thus teaches away from the proposed combination of *Veneklase* and *Jonsson*.

For these and all the reasons discussed in Patent Owner's Response, the cited references fail to teach or suggest claim element [5.5].

D. The Combination of *Veneklase* and *Jonsson* Does Not Teach or Suggest Claim Element [5.6].

As discussed in Patent Owner's Response, Petitioner unambiguously mapped *Veneklase* granting access because the random codes match to the claimed "activates access to the account." *See* Response, p. 35 (citing Pet., p. 41). Having now realized its disadvantage in that mapping, Petitioner seeks to map *Jonsson*'s generation of the "expected response code" to the claimed "activates access to the account." *See* Reply, p. 8 ("POSITA would have understood that the 'expected' response code indicates that the account access is activated because it is awaiting (i.e., expecting) a response."). Thus, Petitioner proceeds in a new direction with a new approach compared to its position in the Petition. *Compare* Pet., p. 41 *with* Reply, p. 8. Patent Owner respectfully submits that Petitioner should be held to its original mapping.

Regarding the claimed "predetermined amount of time," Petitioner argues "a POSITA would have understood that this claim limitation simply means any predetermined period after activation." Reply, p. 9 (citing Ex. 1024, ¶19). Neither Petitioner nor Petitioner's Expert cite to any part of the '658 specification to support their construction. *See* Reply, pp. 7-10; Ex. 2024, ¶¶19-21. That is improper because the words of a claim "are generally given their ordinary and customary

meaning.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc). The “ordinary meaning” of a term “is its meaning to the ordinary artisan after reading the entire patent.” *Id.* at 1321 (emphasis added). The specification “is the single best guide to the meaning of a disputed term.” *Id.* at 1315 (cleaned up). Accordingly, Petitioner’s construction should be disregarded. For the reasons discussed in the Response, Patent Owner maintains the claimed “predetermined amount of time” should be construed as the entire window between activation and deactivation of the account.

Petitioner makes several references to the “predetermined period of time” disclosed by *Veneklas*. See Reply, pp. 9 (“would be governed by Veneklas’s teaching that the password must be ‘received within a predetermined period of time.’”) (emphasis added), 10 (“Veneklas’s teaching that the password must be ‘received within a predetermined period of time’ . . . this line of attack completely ignores Veneklas’s teaching that the password must be ‘received within a predetermined period of time.’”) (emphasis added). If Petitioner is mapping *Veneklas*’s “predetermined period of time” to the claimed “predetermined amount of time,” that mapping is flawed. Specifically, *Veneklas*’s “predetermined period of time” starts when *Veneklas*’s system receives the password from the user (i.e., step one in *Veneklas*’s two-step authentication process). See Ex. 1005, 8:40-49. In

contrast, the claimed “predetermined amount of time,” under both sides’ construction, does not start when the system receives a password from the user.

Petitioner says “the predetermined period would include the time from receiving the challenge code (at or after account activation, as discussed above) and the sending of the response code.” Reply, p. 9. Patent Owner disagrees. The claimed “authentication module” deactivates the account upon expiration of the claimed “predetermined amount of time.” Accordingly, the claimed “authentication module” must know when the “predetermined amount of time” expires so that it can deactivate the account. Petitioner and its expert fail to explain how *Veneklase*’s “code compare module” (Petitioner-identified “authentication module”) would know exactly when the user sends the response code (i.e., the expiration of the “predetermined period”) because there is a delay between the user sending the “response code” and the “code compare module” (Petitioner-identified “authentication module”) receiving the “response code.” Accordingly, Petitioner’s mappings are flawed.

Finally, Petitioner argues “Patent Owner alleges that ‘the predetermined period of time’ varies by when the user decides to send back the response code. However, this line of attack completely ignores *Veneklase*’s teaching that the password must be ‘received within a predetermined period of time.’” Reply, p. 10 (internal citations omitted) (citing Response, p. 37). It is unclear what is meant by

“completely ignores.” As discussed above, *Veneklase*’s “predetermined period of time” is not and cannot be the claimed “predetermined amount of time.” Further, different users have different levels of responsiveness. So the time between a user receiving the challenge code and sending the response code is user dependent (*see* Ex. 2003, ¶102), and is not a “predetermined amount of time” as claim element [5.6] requires.

Given the foregoing and all the reasons discussed in Patent Owner’s Response, the cited references fail to teach or suggest claim element [5.6].

IV. GROUND 2 — *KEW* AND *SORMUNENDO* NOT RENDER OBVIOUS INDEPENDENT CLAIMS 1 and 5.

A. The Combination of *Kew* and *Sormunen* Does Not Teach or Suggest Claim Element [5.3].

Patent Owner’s Response argued that *Kew* fails to teach or suggest the claimed “token” because there is no evidence that *Kew*’s “Code A” (Petitioner-identified “token”) is “eventually . . . known to the user,” as Petitioner’s own claim construction requires. *See* Response, pp. 46-47 (quoting Pet., p. 10). Petitioner’s Reply provided no rebuttal to that showing. *See* Reply, pp. 11-16. Thus, *Kew* fails to teach or suggest the claimed “token.” *Sormunen* does not cure the deficiencies of *Kew*, and the Petition does not so allege. *See* Pet., pp. 60-63. Accordingly, the cited references fail to teach or suggest claim element [5.3].

Petitioner argues that either *Kew*'s "user identification code" or *Kew*'s "identity code" is the claimed "passcode." See Reply, pp. 11 ("The Petition identified the User ID/IdentityCode as the 'passcode' limitation."), 12-13 ("both the user identity code (user ID) and the corresponding identity code (identified by the user ID) are used to generate Code B (e.g., password)") (emphasis added). Neither mapping is correct and each is addressed below.

1. *Kew*'s "identity code" is not the claimed "passcode."

The claim language is unequivocal: "the passcode is known to the user." Ex. 1001, 12:29-32. Petitioner is unable to identify any disclosure in *Kew* that the "identity code" is known to the user, as claim limitation [5.3] requires. See Reply, pp. 11-16. Facing that reality, Petitioner fabricates unrealistic scenarios to argue that *Kew*'s "identity code" is known to the user:

a POSITA would have understood that it would be practical for the user [to] know the identity code. For example, if the user were to forget his user ID, the user would need to use the identity code as a back-up verification in order for the system to locate the correct algorithm to produce a password. Otherwise, the user would not be able to access the system and the receiver would need to be reprogrammed.

Reply, pp. 14-15 (internal citations omitted) (emphasis added). Petitioner's only support for that fabrication is a supplemental declaration, which does not cite any evidence, which should be afforded no weight. See Ex. 1024, ¶28; *Xerox Corp., et al. v. Bytemark, Inc.*, IPR2022-00624, Paper 9, pp. 15-16 (P.T.A.B. Aug. 24, 2022)

(Precedential) (declaration is entitled to little weight when it restates petitioner's arguments without any additional supporting evidence). Regardless, Petitioner's reasoning is flawed.

First, Petitioner concedes that *Kew* filed in January 1995. Pet., p. 1. *Kew* discloses that the “identity code is a key for the one-way [encryption] algorithm.” Ex. 1007, 7:20-32. So in Petitioner's scenario, the end user has forgotten his user ID, but somehow remembers an encryption key that was never needed for input before. That is not realistic today or in January 1995. Further, neither Petitioner nor its expert provide any evidence that *Kew*'s system can even accept the “identity code” (i.e., encryption key) as an input from the user “to locate the correct algorithm.” See Reply at 14-15; Ex. 1024, ¶28.

Second, it is unclear why a forgotten user ID in Petitioner's scenario necessarily requires reprogramming the receiver. As disclosed by *Kew*, “[w]hen the user seeks access to the host system 1 via the terminal 2, he enters his user identification code . . . The security server 5 includes a database of all authorised users and their authorised receiver units 6, and identifies the corresponding identity code for the appropriate receiver unit 6.” Ex. 1007, 7:34-8:5. See also *id.*, 11:8-11 (*Kew*'s system “uses the user identification code (USER ID) to access its database to locate the corresponding identity code for the appropriate receiver unit.”). Given those disclosures, Petitioner fails to explain why a new user ID could not simply be

assigned to the user and *Kew*'s database be updated accordingly. There is no need to reprogram the receiver unit; it can keep its stored "identity code."

Accordingly, *Kew* fails to teach or suggest that that the "identity code" (Petitioner-identified "passcode") is known to the user, and thus fails to teach or suggest claim element [5.3].

2. *Kew*'s "user identification code" is not the claimed "passcode."

In several instances, the Petition unambiguously mapped *Kew*'s "identify code" to the claimed "passcode." *See* Pet., p. 60 ("*Kew* discloses . . . a passcode (e.g., identity code)"), pp. 62-63 ("*Kew* teaches . . . a passcode (e.g., identity code)"). Its original expert Declaration did the same. *See* Ex. 1003, ¶136 ("*Kew* discloses . . . a passcode (e.g., identity code)"), ¶140 ("*Kew* teaches . . . a passcode (e.g., identity code)"). Having now realized its disadvantage in that mapping, Petitioner seeks to map *Kew*'s "user identification code" to the claimed "passcode" instead. Patent Owner respectfully submits that Petitioner should be held to its original mapping.

Regardless, *Kew*'s "user identification code" is also not the claimed "passcode." Claim element [5.3] recites, in part "create a new password based at least upon a token and a passcode." Ex. 1001, 12:28-29. The '658 Patent uses the term "password" to refer to the combination of at least the "passcode" and a "token." Ex. 1001, 4:52-53 ("In the preferred embodiment, the user 108 combines the token

156 with the passcode 154 to form a password 158.”). For example, if the passcode is “abcd” and the token is “1234,” the password could be “abcd1234” or “1234abcd.” *See id.* at 4:54-56, Fig. 2A (“Your password is your passcode followed by a valid token.”) (emphasis added). Petitioner’s Expert concedes that is how the ’658 Patent uses the term “password.” *See* Ex. 1003, ¶26. The Petition itself concedes that is how the ’658 Patent uses the term “password.” *See* Pet., p. 3. In its Claim Construction Order dated Oct. 31, 2023 (i.e., after the deadline for filing Patent Owner’s Response), the United States District Court for the Eastern District of Texas reached the same conclusion: “until the passcode and token are combined, there is no password.” Ex. 2006, p. 15. But *Kew*’s “user identification code” (Petitioner-identified “passcode”) is never combined with *Kew*’s “Code A” (Petitioner-identified “token”) to generate *Kew*’s “Code B” (Petitioner-identified “password”). Accordingly, *Kew*’s “user identification code” (Petitioner-identified “passcode”) is not the claimed “passcode.”

3. *Kew*’s “user identification code” and *Kew*’s “identity code” are different.

Petitioner’s Reply argues that *Kew* suggests that its “user identification code” and “identity code” are the same. *See* Reply, pp. 15-16. That is not true.

Kew discloses that the “identity code is a key for the one-way [encryption] algorithm.” Ex. 1007, 7:20-32. *Kew* never discloses that the “identity code” is the

user's name or a PIN. *See id.* In contrast, *Kew* discloses that the “user identification code” may be the user's “actual name or preferably a more secure code such as a PIN.” Ex. 1007, 7:35-8:2. And *Kew* never discloses that the “user identification code” is an encryption key. *See id.* Accordingly, *Kew*'s “user identification code” and *Kew*'s “identity code” are not the same.

Further, *Kew*'s system “uses the user identification code (USER ID) to access its database to locate the corresponding identity code for the appropriate receiver unit.”). Ex. 1007, 11:8-11 (emphasis added). *See also id.*, 7:34-8:5 (“When the user seeks access to the host system 1 via the terminal 2, he enters his user identification code . . . The security server 5 includes a database of all authorised users and their authorised receiver units 6, and identifies the corresponding identity code for the appropriate receiver unit 6.”) (emphasis added). Accordingly, *Kew*'s “user identification code” is used to lookup, within a database, the appropriate “identity code.” If *Kew*'s “user identification code” and “identity code” were the same, the “identity code” would be known as soon as the “user identification code” is known, and there would be no need to look it up. Accordingly, *Kew*'s “user identification code” and *Kew*'s “identity code” are not the same.

Petitioner's Reply argues “Claim 1 of *Kew* suggests that [the “user identification code” and the “identity code”] can be the same, [because] the ‘input user identification code’ is performing the same function as the identity code of

identifying the transformation algorithm to generate Code B.” Reply, p. 15. Claim 1 makes no such suggestion. It merely recites that the “user identification code” identifies a transformation algorithm. Ex. 1007, 15:3-12 (“a transformation algorithm identified by the input user identification code.”) (emphasis added). Claim 1 does not even recite the “identity code.” *See id.* And as shown above, *Kew*’s “identity code” is an encryption key, while *Kew*’s “user identification code” is not. Accordingly, *Kew*’s “user identification code” and *Kew*’s “identity code” are not the same.

For these and all the reasons discussed in Patent Owner’s Response, the cited references fail to teach or suggest claim element [5.3].

B. The Combination of *Kew* and *Sormunen* Does Not Teach or Suggest Claim Element [5.6].

As discussed in Patent Owner’s Response, Petitioner unambiguously mapped *Kew* granting access because “Code B” and “Code C” match to the claimed “activates access to the account.” *See* Response, p. 49 (citing Pet., p. 67). Having now realized its disadvantage in that mapping, Petitioner seeks to map *Kew*’s generation of “Code B” to the claimed “activates access to the account.” *See* Reply, p. 17 (“a POSITA would have understood that *Kew*’s generation of Code B is ‘activating access’ to the account.”). Thus, Petitioner proceeds in a new direction with a new approach compared to its position in the Petition. *Compare* Pet., p. 67

with Reply, p. 17. Patent Owner respectfully submits Petitioner should be held to its original mapping.

Further, claim element [5.6] recites “activates access to the account in response to the password.” Ex. 1001, 12:41-43. Based on the plain language of the claim, because “activat[ing] access to the account” is done “in response to the password,” “activat[ing] access to the account” must be done after the password is generated. Accordingly, contrary to Petitioner’s contentions, a POSITA would not have understood that *Kew*’s generation of Code B is “activating access” to the account.

Petitioner spends multiple pages alleging that *Kew* discloses two methods for implementing time-bound security. *See* Reply, pp. 17-22. Each method is addressed below.

The alleged first method for implementing time-bound security limits the lifetime of “Code C” to the “predetermined length of time” (e.g., five minutes) *Kew*’s “receiver unit” is enabled to display Code C. *See* Reply, pp. 17-22. According to Petitioner, “a POSITA would have understood that the security sever of *Kew* would know what the ‘predetermined length of time’ is in order to no longer accept Code C when it is not displayed.” Reply, p. 20. *Kew*’s “security server is waiting for entry of Code C and will not allow access after the display period has expired, i.e., the receiver no longer displays Code C . . . the ‘predetermined length of time’ that the

receiver is enabled to display Code C is a limit that determines the deactivation of the account access for Code C in the security server.” Reply, pp. 19-20. Petitioner is misguided.

Even if *Kew*’s “security server” knows the “predetermined amount of time” (e.g., five minutes) (i.e., display period), both Petitioner and its expert fail to explain how *Kew*’s “security server” knows when *Kew*’s “receiver unit” starts displaying *Kew*’s “Code C.” See Reply, pp. 19-20; Ex. 1024, ¶¶35-37. Again, *Kew*’s “receiver unit” cannot display “Code C” until after *Kew*’s “receiver unit” has both received “Code A,” via *Kew*’s paging system, and calculated “Code C” based on the received “Code A.” See Ex. 1007, 8:12-9:3. Petitioner identifies no mechanism for *Kew*’s receiver unit to signal *Kew*’s security server that it is has started displaying “Code C.” See Reply, pp.18-20. Additionally, or alternatively, Petitioner and its expert fail to explain how *Kew*’s “security server” knows when *Kew*’s “receiver unit” stops displaying *Kew*’s “Code C,” and thus knows when to deactivate access to the account. See Reply, pp. 19-20; Ex. 1024, ¶¶35-37. As conceded by Petitioner, “the receiver of *Kew* does not have a mechanism to signal security server 5 to deactivate access to the account in response to expiration of the ‘predetermined length of time’ on the receiver display.” Reply, p. 20 (emphasis added). Accordingly, that first method for implementing time-bound security does not exist in *Kew*.

The alleged second method for implementing time-bound security limits the

lifetime of “Code A.” *See* Reply, pp. 21-22. According to Petitioner, “once Code A is sent by the security server to the receiver, the user is alerted and only has a ‘predetermined period’ to enter the second PIN to allow Code C to be generated and displayed.” Reply, p. 21 (citing Ex. 1007, 3:14-23). Petitioner is mischaracterizing *Kew*. *Kew* discloses that the user can activate the “receiver unit” before or after he enters his “user identification code” into the terminal. *See* Ex. 1007, 8:25-33 (“After or before entering his identification code into the terminal 2, the user also activates the receiver unit 6 by entering a second user identification code”). Accordingly, *Kew* discloses that the user can activate the “receiver unit” before it even receives “Code A.” *See id.* The “predetermined period” is merely how long *Kew*’s “receiver unit” remains activated once it has been activated. As disclosed by *Kew*, it would be a security risk to have the “receiver unit” permanently activated in case an unauthorized user acquires possession of it. *See* Ex. 1007, 3:14-23. Accordingly, that second method for implementing time-bound security does not exist in *Kew*.

Even if one or both methods for implementing time-bound security did exist in *Kew*, Petitioner still fails to explain how they meet the requirements of claim element [5.6]. Again, claim element [5.6] requires that an “authentication module” activate access to the account, which starts a “predetermined amount of time,” and that the “authentication module” deactivate the account upon expiration of the “predetermined amount of time.” Ex. 1001, 12:41-45. *See also* Response, pp. 33-

35.

To the extent that Petitioner is mapping the “predetermined length of time” that *Kew*’s “receiver unit” is enabled to display “Code C” to the claimed “predetermined amount of time,” that mapping is flawed. As discussed above, *Kew*’s “security sever” (Petitioner-identified “authentication module”) has no way of knowing when *Kew*’s “receiver unit” stops displaying “Code C,” and thus has no way of knowing when to deactivate the account. Further, *Kew*’s “predetermined length of time” starts when *Kew*’s “receiver unit” starts displaying “Code C.” In contrast, the claimed “predetermined amount of time” starts with activating access to the account.

To the extent that Petitioner is mapping the “predetermined period” that *Kew*’s “receiver unit” remains activated to the claimed “predetermined amount of time,” that mapping is also flawed. *Kew*’s “security sever” (Petitioner-identified “authentication module”) has no way of knowing when the “predetermined period” will end (i.e., the receiver unit is no longer activated), and thus has no way of knowing when to deactivate the account. Further, *Kew*’s “predetermined period” starts when *Kew*’s “receiver unit” is activated. In contrast, the claimed “predetermined amount of time” starts with activating access to the account.

For the foregoing reasons, and all the reasons discussed in Patent Owner’s Response, the cited references fail to teach or suggest claim element [5.6].

C. The Combination of *Kew* and *Sormunen* Does Not Teach or Suggest Claim Element [1.2].

Patent Owner's Response argued that Petitioner's proposed combination changes *Kew*'s principle of operation and thus there is no motivation to combine. *See* Response, 56-58. Petitioner's Reply provided no rebuttal to that showing. *See* Reply, pp. 23-24.

Patent Owner's Response also argued that Petitioner's proposed combination "requires transmitting *Kew*'s 'user identification code' twice, on two separate devices, for a single session with *Kew*'s system" and that double transmission "increased the likelihood of [*Kew*'s "user identification code"] being intercepted." Response, pp. 58-59. Petitioner's Reply argued that "*Kew* specifically allows for communication between the terminal and the receiver, which would allow for a single entry on the receiver." Reply, p. 23 (citing Ex. 1007, 9:27-31) (emphasis added). Petitioner is misguided.

First, Patent Owner warned against double transmission of *Kew*'s "user identification code," not double entry. *See* Response, pp. 58-59.

Second, even if a single entry of *Kew*'s "user identification code" on *Kew*'s "receiver unit" is shared with *Kew*'s "terminal," the proposed combination still requires two transmissions of *Kew*'s "user identification code" to *Kew*'s "security system:" (1) when *Kew*'s "receiver unit" (Petitioner-identified "personal

communication device”) requests *Kew*’s “Code A” (Petitioner-identified “token”), and (2) when the user seeks access via the terminal. *See* Ex. 1007, 7:10-35, 8:25-26. *See also* Response, pp. 58-59 (citing Ex. 2003, ¶¶128-129). Although not entirely clear, Petitioner seems to be arguing that transmission (2) is not required. *See* Reply, p. 23. But Petitioner and its expert fail to explain how *Kew*’s system, without transmission (2), would know which terminal of the many terminals should be monitored for *Kew*’s “Code C” (i.e., Petitioner-identified “password” from user). *See* Reply, p. 23; Ex. 1024, ¶¶40-41.

For the foregoing reasons, and all the reasons discussed in Patent Owner’s Response, the cited references fail to teach or suggest claim element [1.2].

V. CONCLUSION

For the foregoing reasons, and all the reasons discussed in Patent Owner’s Response, Petitioner has not established that the cited references render any of the challenged claims unpatentable.

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. § 42.24(d), I hereby certify that the foregoing Patent Owner's Sur-Reply contains 5,538 words as measured by the word processing software used to prepare the document, excluding the cover page, signature block, and portions exempted under 37 C.F.R. § 42.24(a) or (b).

DATED: March 1, 2024

Respectfully submitted,

By: /John Wittenzellner/

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

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6, the undersigned certifies that on March 1, 2024, the foregoing document was served on counsel of record for Petitioner by filing this document through the End-to-End System, as well as via electronic mail to counsel of record for Petitioner at the following addresses: Timothy J. Murphy (tj@unifiedpatents.com), Jordan M. Rossen (jordan@unifiedpatents.com), How-Ying Liou (aliou@jonesday.com), Vishal Khatri (vkhatri@jonesday.com), Matthew Johnson (mwjohnson@jonesday.com), and Evan Tassis (etassis@jonesday.com).

Respectfully submitted,

By: /John Wittenzellner/

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