

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, LLC,
Petitioner,

v.

DYNAPASS IP HOLDINGS LLC,
Patent Owner.

IPR2023-00425
Patent 6,993,658

PETITIONER'S REPLY

TABLE OF CONTENTS

I. INTRODUCTION	1
II. CLAIM CONSTRUCTION.....	1
III. GROUNDS	2
A. Veneklasé and Jonsson.....	2
1. Limitation [5.3]	2
2. Limitation [5.4]	5
3. Limitation [5.5]	6
4. Limitation [5.6]	7
B. Kew and Sormunen.....	11
1. Limitation [5.3]	11
2. Limitation [5.6]	16
3. Limitation [1.2]	23
IV. THE BOARD HAS JURISDICTION.....	24
V. CONCLUSION	24

EXHIBIT LIST

Exhibit No.	Description
1001	U.S. Patent 6,993,658
1002	Prosecution History File of Application 09/519,829
1003	Declaration of Bruce McNair (¶¶1-168)
1004	Curriculum Vitae of Bruce McNair
1005	European Patent Application No. 084451 to Veneklasé (“ <i>Veneklasé</i> ”)
1006	PCT Patent Publication No. WO 96/00485 to Jonsson (“ <i>Jonsson</i> ”)
1007	PCT Patent Publication No. WO 95/19593 to Kew (“ <i>Kew</i> ”)
1008	PCT Patent Publication No. WO 97/31306 to Sormunen (“ <i>Sormunen</i> ”)
1009	Li Gong, “Optimal Authentication Protocols Resistant to Password Guessing Attacks,” Proceedings The Eighth IEEE Computer Security Foundations Workshop, 1995, pp. 24-29, doi: 10.1109/CSFW.1995.518549.
1010	U.S. Patent 3,938,091
1011	IETF RFC2289, “A One-Time Password System,” February 1989, available at https://www.rfc-editor.org/rfc/rfc2289.html
1012	U.S. Patent 5,276,444

1013	S.A. Sherman, R. Skibo, R.S. Murray, "Secure Network Access Using Multiple Applications of AT&T's Smart Card," AT&T Technical Journal, September/October 1994
1014	Lt. Gen. Charles R. Myers, "Vietnam Studies: Division-Level Communications, 1962-1973", US Department of the Army, 1982, Ch. 8, retrieved from https://history.army.mil/catalog/pubs/90/90-11.html December 13, 2022.
1015	Z. J. Haas and S. Paul, "Limited-lifetime shared-access in mobile systems," Proceedings IEEE International Conference on Communications ICC '95, 1995, pp. 1404-1408 vol.3, doi: 10.1109/ICC.1995.524434
1016	Mobivity, A Brief History of Text Messaging, Sept. 27, 2012, available at https://www.mobivity.com/mobivity-blog/a-brief-history-of-text-messaging
1017	Declaration of Kevin Jakel (§§115)
1018	Microsoft Computer Dictionary (5th ed. 2002)
1019	U.S. Patent 7,058,974
1020	U.S. Patent 5,559,505
1021	"Viet Nam Studies – Division-Level Communications 1962-1973," Department of the Army, CMH PUB 90-11, 1982.
1022	"Recent-secure authentication: enforcing revocation in distributed systems," <i>Proceedings 1995 IEEE Symposium on Security and Privacy</i> , Oakland, CA, USA, 1995, pp. 224-235, doi: 10.1109/SECPRI.1995.398935
1023	"A class of flexible and efficient key management protocols," <i>Proceedings 9th IEEE Computer Security Foundations Workshop</i> , Kenmare, Ireland, 1996, pp. 2-8, doi: 10.1109/CSFW.1996.503685

1024	Supplemental Declaration of Bruce McNair
------	--

TABLE OF AUTHORITIES

Cases

<i>Apple, Inc. v. Gesture Tech. Partners, LLC</i> , IPR2021-00922, Paper 26 at 25 (Nov. 28, 2022)	24
<i>Bayer Pharma AG v. Watson Labs, Inc.</i> , 874 F.3d 1316, 1327 (Fed. Cir. 2017).....	3
<i>In re Baird</i> , 16 F.3d 380, 383 (Fed. Cir. 1994)	2
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Matal</i> , 868 F.3d 1013, 1017 (Fed. Cir. 2017).....	2
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303, 1323 (Fed. Cir. 2005) (en banc)).....	1, 7
<i>Sony Corp. v. Iancu</i> , 924 F.3d 1235, 1239-41 (Fed. Cir. 2019).....	24

I. INTRODUCTION

Patent Owner's ("PO") response recycles previously rejected arguments and fails to understand the application of the prior art from the perspective of a POSITA. When the prior art is properly considered in its entirety including what it reasonably suggests to a POSITA, claims 1 and 3-6 ("challenged claims") should be canceled.

II. CLAIM CONSTRUCTION

Despite Patent Owner's previous representation that "claim construction is not necessary...", Patent Owner now seeks to import a district court construction that does not affect the grounds of unpatentability. In particular, Patent Owner seeks to import a construction of "activates access to the account in response to the password" to mean "activates access to the account in response to *the creation of* the password." Response, 11. However, PO's proposed construction improperly attempts to import limitations from the specification into the claims, and should be rejected. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (en banc).

Nonetheless, this construction has no bearing on the patentability of the challenged claims at least because, as demonstrated below, the prior art cited in the Petition renders the challenged claims obvious, even under the district court's construction. Accordingly, a construction of this term is not necessary to resolve

this proceeding. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Matal*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

III. GROUNDS

As an initial matter, the Response fails to identify or consider the level of skill in the art. This is no small oversight, as the analysis of the prior art applies a rigid, robotic approach that fails to consider what the teaching of the prior art “fairly suggests” to a POSITA. *See In re Baird*, 16 F.3d 380, 383 (Fed. Cir. 1994) (“[A] reference must be considered not only for what it expressly teaches, but also for what it fairly suggests.”) As set forth below, when the prior art is considered to properly include what it would “fairly suggest” as well as what is expressly disclosed, a POSITA would have found the challenged claims obvious.

A. Veneklas and Jonsson

The combination of Veneklas and Jonsson renders obvious the system of claim 5 when the references are properly considered from the perspective of a POSITA.

1. Limitation [5.3]

PO’s asserts that the proposed modification would “violate *Veneklas*’s principle of operation” by eliminating the double entry of Veneklas’s password, which PO asserts is a “two-step authorization.” Response, 18. PO also argues that there is no evidence that “the security of [the] proposed combination is superior to

the existing multi-layer/level security in *Veneklase*.” *Id.*, 19-20. The Board previously rejected these arguments, and should again. Paper 9, 17-18.

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 have been inferior or that it would not work for Veneklase’s stated goal to “ensure that only authorized users gain access to a computer system.” EX1005, 3:31-33. Indeed, 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. Pet., 31-34. PO admits that requiring entry of the passcode once provides enhanced security over entering the passcode multiple times. Response, 59. Nonetheless, superiority is not a requirement for a finding of obviousness. *Bayer Pharma AG v. Watson Labs, Inc.*, 874 F.3d 1316, 1327 (Fed. Cir. 2017) (that “better alternatives exist in the prior art does not mean that an inferior combination is inapt for obviousness purposes.”)

PO also argues that the proffered modification would somehow decrease security by eliminating Veneklase’s notification that a hacker was seeking access to the system with the password. Response, 20. However, this argument is belied by the fact that the combination would still alert the user that someone is attempting to access the account. EX1024, ¶6. In particular, the combination would require the

user to enter the user input (e.g., PIN) in response to the receipt of the challenge code. Thus, the user would know that a hacker was seeking access to the account by receiving a challenge code without requesting one. *Id.* Also, as explained in the Petition, the proffered combination would require access to the user’s device, which augments the security of the system by preventing SIM swapping, and negates any concerns over a hacker knowing a password. Pet., 32. That is, the hacker would need to know the password **and** have the user’s actual device in order to gain access to the system. *Id.* Put simply, the proposed modification alters the method of operation, but does not destroy the intended purpose of providing security.

PO also argues that the modification would be “more prone to Denial of Service (DoS) attacks...” Response, 21. However, PO does not explain or offer any evidence to support this assertion other than the parroting of its expert. A DoS attack was known at the time of the ’658 patent to be:

characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. DoS attacks are aimed at devices and networks with exposure to the Internet. Their goal is to cripple a device or network so that external users no longer have access to network resources. **Without hacking password files or stealing sensitive data**, a denial-of-service hacker simply fires up a program that will generate enough traffic to a particular

site that it denies service to the site's legitimate users.

EX1019, 1:14-23.¹ Patent Owner's own evidence confirms this understanding.

EX1018 (corresponding to EX2005), 173. Thus, the combined system would not be "more prone" to DoS attack at least because a DoS attack is not dependent on knowing a password. EX1024, ¶¶7-9. As such, like Jonsson and the '658 Patent, Veneklas is susceptible to repeated requests for access from a DoS attack. *Id.* Further, PO's expert admits that Veneklas does not solve the problem of DoS attacks, stating, without explanation, that Veneklas's system is somehow "less susceptible."² EX2003, ¶90. Thus, a POSITA would not be discouraged from combining Veneklas's system with the teachings of Jonsson based on any possibility of increased DoS attacks. EX1024, ¶¶7-9. Accordingly, PO's theory regarding DoS attacks is not credible and should be disregarded in the obviousness analysis.

2. Limitation [5.4]

PO reiterates its previously rejected argument that the modification renders Veneklas inoperable. Response, 25. As noted in the Institution Decision, the Petition relies on the combination of Veneklas and Jonsson to identify the device

¹ Unless otherwise indicated, all emphasis is added.

² This is a notable exception to the expert's nearly verbatim restatement that is conspicuously absent from the PO Response.

in response to the request for authorization as described in Jonsson. Paper 9, 21.

PO alleges that the motivation to combine is flawed because the combination still has two steps. However, 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 Veneklas. Pet., 30-32.

PO again alleges that Jonsson's system is more vulnerable to DoS attacks because the authorization request is not a password. Response, 28. As discussed above, this theory is without merit at least because a DoS attack is an attempt to overwhelm the authorization mechanism through repeated requests. EX1024, ¶¶7-9. Thus, the use of a password instead of another means of requesting access is not relevant to preventing or minimizing a DoS attack. *Id.*

3. Limitation [5.5]

PO reiterates its previously rejected arguments for this limitation. As noted in the Institution Decision, Jonsson's pager is capable of modification including the execution of algorithms. In an attempt to rebut this, PO alleges that Veneklas'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. Nonetheless, this argument is directly contradicted by Jonsson's disclosure, as noted by the Board, "the capacity for performing the necessary calculations exists in

conventional cellular telephones and personal communication units [(i.e., pagers)], allowing the present invention to be implemented through software.” Paper 9, 22, citing EX1006, 7:21-31.

PO attempts to distinguish from this clear teaching by citing the preceding sentence describing a “preferred embodiment” where the personal unit is a separate unit minimizing the need for customization. Response, 31. However, 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. EX1024, ¶13. Further, Veneklas already discloses that its pager unit executes algorithms. EX1005, 9:26-10:11. Thus, a POSITA would have understood that the pager of Veneklas was capable of performing the algorithms of Jonsson.

4. Limitation [5.6]

First, Patent Owner alleges that Veneklas does not activate access in response to the “creation of the new ‘password’.” Response, 35. However, the claim does not include the language “creation of” or any variation thereof. Thus, PO’s attempts to import unclaimed limitations from the specification should be rejected. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (en banc)).

Nonetheless, the combination of Veneklas and Jonsson discloses this limitation even under the court’s interpretation.

Patent Owner is taking the position that “activates access” is something that happens when the user actually accesses the account. However, access to the account has to be activated in order for the newly created password to work and allow access to the account. EX1024, ¶¶15-16. In other words, the account cannot be used when the account is deactivated. As Petitioner’s expert clarifies, not activating access to the account when generating a new password would undermine the purpose of generating a new password, i.e., accessing an account. *Id.*

Jonsson discloses creating “an expected response code,” (e.g., password), at which point access to the account is activated, and access is granted when the “expected response code” matches the received response code. Ex.1006, 10:2-5. In particular, a 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. EX1024, ¶17. As such, Jonsson teaches activating access to the account in response to the creation of the password under the district court’s interpretation.

In addition, Jonsson discloses that “the challenge code and the response is unique for each transaction.” EX1006, 3:16-18. As such, a POSITA would have understood that account access is not activated prior to the sending of the challenge code to the user and the creation of the expected response code (e.g., new password) at least because prior response codes would not have worked. EX1024, ¶18. That is, until the unique challenge code and unique expected response code

are created and sent for a particular transaction, there is no access to the account.

Id.

Second, Patent Owner alleges that the claimed predetermined amount of time is the timeframe between activation and deactivation of the account.

Response, 36. However, as previously noted by the Board, Patent Owner mistakes the “predetermined amount of time after activating the account” to mean the entire period after account access is activated. Paper 9, 25. Rather, a POSITA would have understood that this claim limitation simply means any predetermined period *after* activation. EX1024, ¶19. In the combined system of Veneklas and Jonsson, 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, which would be governed by Veneklas’s teaching that the password must be “received within a predetermined period of time.” EX1005, 8:40-49; EX1024, ¶19.

Third, Patent Owner alleges that “because the Petition alleges that the “predetermined period of time” begins with “receipt of the token (e.g., randomly generated challenge code)” by “pager 420,” it would be the “personal communication device,” not the “authentication module” (i.e., “code compare module 416” in the “host computer”) that activates access to the account.”

Response, 36. This is again based on a misunderstanding of the claim limitation that the predetermined amount of time must include the entire time from activation

of the account to deactivation of the account. EX1024, ¶20. However, this is simply not what the claim recites. Rather, the claim recites “deactivates the account *within* a predetermined amount of time *after* activating the account.” Thus, the predetermined amount of time begins at some point after activation. *Id.*

Accordingly, this limitation is met by Veneklasé’s teaching that the password must be “received within a predetermined period of time” (EX1005, 8:40-49) applied to Jonsson’s sending of the response code after receiving the challenge code.

EX1005, 8:40-49; EX1024, ¶20. Thus, the “authentication module” (i.e., “code compare module 416” in the “host computer”) is responsible for account deactivation. *Id.*

Finally, Patent Owner alleges that “the predetermined period of time” varies by when the user decides to send back the response code. Response, 37. However, this line of attack completely ignores Veneklasé’s teaching that the password must be “received within a predetermined period of time.” EX1024, ¶21. As explained above, the combination of Veneklasé and Jonsson meets the deactivation limitation. EX1005, 8:40-49; EX1024, ¶21.

For the foregoing reasons, as well as the reasons set forth in the Petition, the combination of Veneklasé and Jonsson renders claim 5 obvious.

B. Kew and Sormunen

PO makes several arguments in an attempt to distinguish from the combination of Kew and Sormunen. Again, PO's analysis fails to understand and apply the teachings of the cited references from the perspective of a POSITA.

1. Limitation [5.3]

The Petition identified the User ID/IdentityCode as the “passcode” limitation. Pet., 60-63. The reason for this is simple, as the disclosure of Kew requires the use of a user-known “identification code” to allow for the identification of the correct “identity code,” which is used to generate the password. EX1024, ¶23. In particular, a POSITA would have understood that the “identity code” “corresponds” to a user-known identification code, which is entered by the user during the authentication process. EX1007, 3:1-6; 8:2-9. For example, Kew states:

When the user **enters his user identification code**, the host computer system identifies the corresponding transformation algorithm in a database from the code and transforms the random code (Code A) to a new Code B in such a manner that the Code C, produced by the user's receiver from the transmitted code, will be identical to Code B with which it is compared. Thus, only a user both with knowledge of the user identification code and holding the corresponding receiver can gain access to the host

system.

The transformation algorithms associated with each receiver may be completely different, or may be the same base algorithm which is convoluted with a **code corresponding to the user's identification code** so as to generate characteristic transformed codes.

EX1006, 2:28-3:6.

When the user seeks access to the host system 1 via the terminal 2 , **he enters his user identification code**. This code may take any suitable form, for example his actual name or preferably a more secure code such as a PIN. 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. **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**. In this way a transformed code (Code B) is produced.

EX1006, 7:34-8:10.

A POSITA would have readily understood that both the user ID and the “corresponding identity code” are used to generate a password in the event that they are not identical. EX1024, ¶24. Thus, 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). A POSITA would have understood that the “corresponding identity code” is linked with the user ID such that the user ID (known to the user) is necessary to identify the identity code in instances when they are not the same. *Id.* Thus, in order for the process of Kew to function, the password (Code B) must be “based on” at least the user ID provided by the user. *Id.*

This process is illustrated Fig. 2 of Kew, reproduced below:

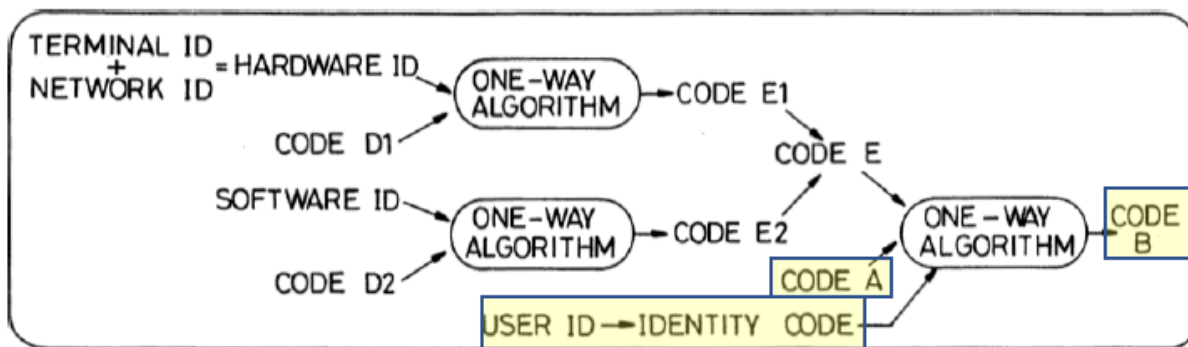


FIG. 2 shows how new password Code B is created based on both the User ID/Identity Code (passcode) and randomly generated Code A. A POSITA would have understood that the User ID is involved in the generation of the password, as the process of generating Code B cannot begin without the User ID to identify the correct algorithm associated with the Identity Code of the device. EX1024, ¶26. Thus, a POSITA would have understood that the password generated by Kew is “based on” the User ID at least because it cannot be generated without out the User

ID, and is also “based on” the identity code (when it is not identical to the User ID) because that is what is used to identify the algorithm used by the receiver. *Id.*

PO also asserts that “identity code” would not be known to the user.

However, PO’s arguments relate to the reprogramming of the receiver and do not support a conclusion that the identity code would not be known to the user.

EX1024, ¶27. The programming of the receiver and storage of the identity code in the EPROM is not relevant to whether the user has knowledge of the identity code.

Id. Further, the reprogramming of the EPROM using ultraviolet light is similarly irrelevant to whether the user knows the identity code. *Id.* EPROM means

“erasable programmable *read*-only memory.” EX2006. This meaning says nothing about who can read the memory, just that it cannot be written to (without having been erased using ultraviolet light). EX1024, Nothing about storing the “identity code” in EPROM prevents the user from knowing its contents or value. *Id.* Indeed, as the name indicates, EPROM is necessarily readable. *Id.*

In addition, Kew does not limit its disclosure to requiring that the identity code is unknown to the user, and PO does not give any reason why the identity code would be secret or hidden from the user. EX1024, ¶28. Rather, a POSITA would have understood that it would be practical for the user know the identity code. *Id.* 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. *Id.* Otherwise, the user would not be able to access the system and the receiver would need to be reprogrammed. *Id.* As noted by PO, reprogramming the EPROM requires exposing the chip to ultraviolet light, which is a process that would be impractical for a layperson user. *Id.* Further, changing the identity code would also require updating the database to also include the new identity code. *Id.* As such, a POSITA reading Kew would not have concluded that the identity code was a secret, as such an interpretation would be impractical and provide no benefit to the user. *Id.* Instead, a POSITA would have understood that it would have been beneficial for the user to know the identity code of the device to avoid the burdensome process of reprogramming the receiver in the event that the user forgets the PIN.

Kew is not limited such that the user identification code must be different from the identity code. EX1024, ¶29. Rather, Claim 1 of Kew suggests that they can be the same, as the “input user identification code” is performing the same function as the identity code of identifying the transformation algorithm to generate Code B. *Id.*

1. A method of preventing unauthorised access to a host computer system (1) by a user at a remote terminal (2) comprising the steps of accepting a user identification code input to the terminal by the user; generating a random code (Code A) ; **subjecting Code A to a transformation**

characteristic of a transformation algorithm identified by the input user identification code so as to generate a transformed code (Code B) ; transmitting Code A via a paging system (7) , to a receiver (6) held by the user, the receiver (6) comprising transformation means adapted to transform the received Code A to a second transformed Code C...

EX1007, 15:1-16. Thus, claim 1 of Kew supports the user ID as the same as the identity code. EX1024, ¶29.

In view of the foregoing, the combination of Kew and Jonsson discloses limitation [5.3].

2. Limitation [5.6]

a) “activates access to the account in response to the password”

Kew discloses that access to the account is activated in response to the password, as claimed. PO relies on a district court interpretation of this limitation to include the words “the creation of” such that the court’s interpretation of this limitation is “activates access to the account in response to *the creation of* the password.” Kew discloses this limitation even under the court’s interpretation. As discussed above regarding Ground 1, it appears that PO is taking the position that “activates access” is something that happens before entry of the password. However, access to the account has to be activated in order for the created

password to work. EX1024, ¶30. In other words, the account cannot be used when the account is deactivated. *Id.*

Kew discloses the “activates access” limitation under PO’s interpretation because the creation of the new password (Code B) is activating access to the account. EX1024, ¶31. Kew sends Code A to the receiver so that it can be transformed into Code C. The security server then compares Code C with Code B to allow access to the account if the two match, which cannot happen if the account is not already activated, i.e., if Code B has not already been generated. EX1007, 2:27-34. EX1024, ¶31.

Thus, a POSITA would have understood that Kew’s generation of Code B is “activating access” to the account.

b) “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”

PO alleges that Kew does not disclose that the “security server 5” deactivates the account. Response, 53. In particular, PO alleges that “account access remains active indefinitely after Code A has been transmitted.” This is another example of PO not applying the perspective of a POSITA to the disclosure of Kew. A POSITA would have understood that Kew’s disclosure of limiting the time for displaying Code C is an example of the well-known concept of time-bound access. EX1003, ¶49; EX1024, ¶32.

As Petitioner’s expert explains, the concept of the “timeliness” or “lifetime” of information or its “freshness” was well-known for cryptographic keys as well as authentication systems. EX1024, ¶33. The longer an authentication parameter or cryptographic key is in use and as more information becomes dependent on its security, the greater the chance of compromise of that information. *Id.* Thus, specific mechanisms to ensure the “freshness” or “timeliness” of cryptographic keys or challenge-response values were well-known before the ’658 patent. As such, time-based authorization was well-known prior to the ’658 patent. *Id.*

Kew teaches time-based access. EX1024, In particular, Kew teaches that the receiver is only enabled to display Code C for a limited time, e.g., 5 minutes. EX1007, 8:33-9:3. A POSITA would have understood from this disclosure that Code C was only valid for this limited time, as allowing Code C to be valid indefinitely, as PO suggests, would compromise security as was well-known prior to the ’658 Patent’s priority date. EX1024, ¶34. A POSITA would have understood that sending code A to be transformed by the receiver would have included a time limitation, as this was commonplace. For example, Kew discloses:

this transformed Code C is then displayed to the user on a display means 9, preferably a liquid crystal display, for a **predetermined length of time such as five minutes.**

The terminal 2, **at the behest of the security server 5 prompts the user to input the transformed Code C**

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

EX1007, 9:1-11. A POSITA would have understood that the “predetermined length of time” was known by both the security server 5 and the receiver. EX1024, ¶35. In particular, Kew indicates that the security server “prompts” the user to enter code C. A POSITA would have understood that a “prompt” in this context is a “displayed text indicating that a computer program is *waiting for input* from the user.” EX1018, 427; EX1024, ¶35. A POSITA would have understood that Kew’s disclosure of the security server’s instruction to prompt the user “to input the transformed code C displayed by the receiver” is an indication that the 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. *Id.* Otherwise, as Petitioner’s expert explains, there would not be any need for the security server to prompt the user to enter Code C, and the user could simply write down Code C and enter it days later to access the account. *Id.* This would be counter to the goal of achieving time-bound access, and a POSITA would not have understood Kew’s disclosure to operate in this manner. *Id.*

Further, Kew discloses that the security server “prompts” entry of the “transformed Code C **displayed by the receiver unit 6.**” EX1007, 9:6-7. A POSITA would have understood that this disclosure meant that the account access was only active while the display was active, otherwise Kew would have simply disclosed entry of “transformed Code C” and not specified that it must be “displayed by the receiver unit 6.” EX1024, ¶36. Thus, a POSITA would have understood that 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. *Id.* As noted by PO, 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. *Id.* Accordingly, a POSITA would have understood that the security server of Kew would know what the “predetermined length of time” is in order to no longer accept Code C when it is not displayed, i.e., it has expired.

Kew also demonstrates time-bound access through the use of a second PIN. EX1024, ¶37. This “additional security” functions by only allowing code A, which is sent by security server 5, to be transformed into Code C during a “predetermined period.” *Id.* PO alleges that this is accomplished by merely locking/unlocking the screen of the receiver unit, and that after the predetermined period, the screen can be unlocked again by use of the second PIN. Response, 54. However, PO’s

interpretation of Kew is based on the faulty premise that Kew's codes are "active indefinitely" EX1024, ¶37. However, this is not how Kew functions, and not how a POSITA would have understood Kew's time-bound access to add security. *Id.* Further, PO overlooks that this disclosure relates to the ability to transform Code A to Code C, and not merely to the ability to display Code C. *Id.*

A POSITA would have understood that Kew's additional time-bound access relates to permitting the algorithm to transform Code A to Code C for a limited time once it is received by the receiver. EX1024, ¶38. This is consistent with the known time-based security solutions as of the priority date of the '658 patent. *Id.* For example, Kew's security server sends Code A to receiver, which alerts the user that the code has been sent by security server. Ex. 1007, 3:31-4:10. The user then enters the second PIN in order to transform Code A to Code C and allow Code C to be displayed so that it can be entered by the user for comparison to Code B. Ex. 1007, 3:14-23. A POSITA would have understood this disclosure to mean that Code A is time-bound. EX1024, ¶38. That is, 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. *Id.* This "additional security" feature is consistent with the time-bound limited display feature discussed above and further demonstrates that Kew's codes are not "active indefinitely." *Id.*

Petitioner's expert demonstrates an exemplary system of Kew using **both** time-based security features would function as follows:

- 1) The user enters the user ID to generate Code A, which is used with the user ID/identity code to generate Code B, which begins the lifetime of Code B for a predetermined 5 minute period.
- 2) Code A is sent to the receiver, which begins the lifetime of Code A for a predetermined period of 5 minutes. The user is alerted to enter his second identification code, which enables Code A to be transformed to Code C and displayed.
- 3) The user must enter Code C while it is displayed during the 5 minute period that the receiver is enabled to generate code C. EX1024, ¶39.

Thus, Kew discloses two methods for implementing time-bound security. The first method limits the lifetime of Code C (and Code B) to the "predetermined length of time" it is able to be displayed for entry and comparison. EX1024, ¶39. The second method enables the receiver to transform Code A to Code C for "predetermined period." *Id.* A POSITA would have understood that this was accomplished by limiting the lifetime of Code A to the "predetermined period." *Id.*

In view of the foregoing, the combination of Kew and Jonsson discloses limitation [5.6].

3. Limitation [1.2]

PO alleges that the proposed modification to Kew with the disclosure of Sormunen would somehow require the entry of Kew's user ID twice. Response, 59. However, POSITA would have understood that modifying Kew's receiver to allow two-way communication by the teachings of Sormunen would not require entering the user ID two times. EX1024, ¶40. In particular, Patent Owner alleges that the user ID would need to be entered first to "identify the terminal" where the user is located, and then again by the modified receiver to request a token. Response, 59. Patent Owner cites Kew at 7:10-18 and 9:5-7 for this alleged requirement. However, Patent Owner misinterprets this disclosure, as it is directed to the identification of the user, and not the terminal. Further, Kew specifically allows for communication between the terminal and the receiver, which would allow for a single entry on the receiver. EX1007, 9:27-31; EX1024, ¶40.

Nonetheless, even if a user were required by the modification to enter the user ID twice, the security of the modified system would still be intact through Kew's time-based security features in order to prevent unauthorized access. EX1024, ¶41. In particular, Kew's "additional security" is effective even in circumstances when the user ID is known by an unauthorized user. EX1007, 3:14-23; EX1024, ¶41. Thus, even under Patent Owner's interpretation requiring a

double transmission of the user ID, the system of Kew is secure against unauthorized access. *Id.*

Patent Owner does not address any other limitations of the challenged claims. Thus, in view of the foregoing, the challenged claims are obvious over the combination of Kew and Jonsson.

IV. THE BOARD HAS JURISDICTION

PO repeats its argument that the Board lacks jurisdiction over expired patents. This same argument has been made *verbatim*, and has been soundly rejected by the Board. *Apple, Inc. v. Gesture Tech. Partners, LLC*, IPR2021-00922, Paper 26 at 25 (Nov. 28, 2022). In particular, the Board found Federal Circuit has confirmed the PTAB's authority to review expired patents. *Id.*, citing *Sony Corp. v. Iancu*, 924 F.3d 1235, 1239-41 (Fed. Cir. 2019). Thus, this *verbatim* argument that has been attempted previously and rejected, should similarly be rejected here.

V. CONCLUSION

For the foregoing reasons, claims 1 and 3-6 should be canceled.

Dated: January 9, 2024

Respectfully Submitted,

/Timothy J. Murphy/
Timothy J. Murphy
Registration No. 62,585

Jordan M. Rossen
Registration No. 74,064

CERTIFICATION UNDER 37 CFR § 42.24(d)

Under the provisions of 37 CFR §42.24(d), the undersigned hereby certifies that the word count for the foregoing Petitioner's Reply excluding the portions exempt under 37 CFR §42.24(a)(1)—totals 5,394 words, which is less than the 5,600 allowed under 37 CFR §42.24(c)(1).

Dated: January 9, 2024

Respectfully Submitted,

/Timothy J. Murphy/
Timothy J. Murphy
Registration No. 62,585

Jordan M. Rossen
Registration No. 74,064

CERTIFICATE OF SERVICE

I hereby certify that on January 9, 2024, I caused true and correct copies of the foregoing **Petitioners' Reply, and Exhibits 1008 through 1024** to be served electronically on correspondence addresses of record:

johnw@wsltrial.com
IPRDYNAPASSWSL@wsltrial.com
tlandis@wsltrial.com
mfagan@wsltrial.com
mmccarthy@wsltrial.com

Dated: January 9, 2024

By: /Ashley F. Cheung/
Ashley F. Cheung
Paralegal
Unified Patents, LLC