

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, LLC

Petitioner

- v. -

DYNAPASS HOLDINGS, LLC

Patent Owner

IPR2023-00425

U.S. Patent 6,993,658

SUPPLEMENTAL DECLARATION OF BRUCE MCNAIR

TABLE OF CONTENTS

I.	Introduction	3
II.	GROUND 1	5
A.	Limitation [5.3] “a control module . . . configured to create a new password based at least upon a token and a passcode”	5
B.	Limitation [5.4] “a communication module configured to transmit the token to the personal communication device through the cell phone network;”	9
C.	Limitation [5.5] “an authentication module configured to receive the password from the user through a secure computer network,”	10
D.	Limitation [5.6] “wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account, such that said account is not accessible through any password via the secure computer network,”	11
III.	GROUND 2	15
A.	Limitation [5.3]- the “passcode”	15
B.	Limitation [5.6] “activates access to the account in response to the password”	20
C.	Limitation [5.6] “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”	21
D.	Limitation [1.2] “receiving a request from the user for a token via the personal communication device, over the second network”	27
IV.	Conclusion	28

I, Bruce McNair, do hereby declare as follows:

I. INTRODUCTION

1. I have been asked to respond to certain opinions in Patent Owner's Response (POR), Paper 13, in this proceeding. As with my previous declaration, EX1003, in forming the opinions expressed in this declaration, I relied upon my education and experience in the relevant field of art and have considered the viewpoint of a Person of Ordinary Skill in the Art ("POSITA"), as of March 6, 2000, the priority date of U.S. Patent 6,993,658 ("the '658 patent"). I have also relied on the following exhibits:

Exhibit No.	Description
1001	U.S. Patent 6,993,658
1002	Prosecution History File of Application 09/519,829
1005	European Patent Application No. 084451 to Veneklasė ("Veneklasė")
1006	PCT Patent Publication No. WO 96/00485 to Jonsson ("Jonsson")
1007	PCT Patent Publication No. WO 95/19593 to Kew ("Kew")
1008	PCT Patent Publication No. WO 97/31306 to Sormunen ("Sormunen")
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
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

II. GROUND 1

2. Patent Owner makes several arguments in an attempt to distinguish from the Veneklasé/Jonsson combination. However, the fundamental error in Patent Owner's analysis is that it fails to understand the cited references from the perspective of a POSITA. As I explained in my previous declaration, EX1003, when the combination of the disclosure of Veneklasé and Jonsson is viewed from the perspective of a POSITA, claim 5 is obvious.

3. Patent Owner disputes the application of Veneklasé and Jonsson to certain limitations of claim 5. I address each of the challenged limitations below.

A. Limitation [5.3] "a control module . . . configured to create a new password based at least upon a token and a passcode"

4. Patent Owner alleges that modifying Veneklasé with the teaching of Jonsson to allow for the transmission of the password only one time would "violate Veneklasé's principle of operation" because the two-step authentication is a "key

feature” of Veneklas. I disagree. The modified system would still allow for multiple levels of security. In particular, the modified system includes entering the PIN (e.g., passcode) only one time after a request for authorization is initiated. However, the entry of the PIN is only done after the receipt of a challenge code, as taught by Jonsson. Thus, the PIN is only entered once into the personal unit 20 and is not transmitted, which prevents interception. Rather, the PIN is entered into the user’s device and a response code is generated based on the received challenge code, [and] the user input (e.g., PIN) .” EX1006, 8:12-14. To be clear, this method is more efficient than the process of Veneklas because it saves the user from having to manually enter both the PIN and the challenge code. That is, the method of Jonsson calculates and sends the response code (e.g., password) after receipt of the challenge code and the single entry of the PIN.

5. While the modification necessarily changes how Veneklas would operate, it still accomplishes Veneklas’s goal of preventing unauthorized access and adds advantages. In particular, I note that incorporating Jonsson’s teaching to only require entry of the PIN to the user’s device provides added security over sending the PIN over a communication channel where it can be intercepted.

6. The portion of Veneklas cited by Patent Owner relates to notifying the user that someone is seeking access to the system with the password. The proposed modification would also notify the user that someone is seeking access

because the user would receive a challenge code (e.g., token), which would alert the user that someone is seeking access to the account.

7. Patent Owner also concludes that the combined system would be “more prone to Denial of Service (DoS) attacks.” This argument is a red herring. For example, a POSITA would have understood a DoS attack as:

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. Patent Owner’s own evidence confirms this understanding:

Computerized assault, usually planned, that seeks to disrupt Web access. A denial of service attack can occur in a number of forms. **The most common form of attack is to overwhelm an Internet server with connection requests that cannot be completed.** This causes the server to become so busy attempting to respond to the attack that it ignores legitimate requests for connections. One example of this type of attack, known as a SYN flood, inundates the server’s entry ports with false connection messages. Another, known as the Ping of Death, sends a ping command with an oversized IP packet that causes the server to freeze, crash, or restart.

Other forms of denial of service attacks include the destruction or alteration of a server's configuration data, such as router information; unauthorized access to physical components of a system; and the sending of large or invalid data that causes a system to crash or freeze. See also packet, Ping of Death, SYN flood.

EX1018, p. 173.

8. The problems of DoS attacks on authentication systems have been known long before either of the prior art references or the patent filing. I have personal experience in addressing the long-known problem of attackers creating a DoS by repeated invalid access attempts. See, e.g., McNair, US Patent 5,559,505 "Security System for Providing Lockout for Invalid Access Attempts," granted September 24, 1996, EX1020. Jonsson does not exacerbate this problem but, in fact, acknowledges the fact that there may very well be invalid access attempts, e.g., in Claim 22 "permitting access to said service only when a result of said comparison of said response code generated by said personal unit to said expected response code is acceptable." The '658 patent only appears to address how to process access requests when the requests are valid. Only in the Background (1:29-31) does the '658 patent even briefly acknowledge the actions of hackers guessing passwords. Nowhere, not in the flow chart diagrams, in the written description, or claims does it address the necessary system actions when an invalid access attempt is made, thus failing to consider or address any potential DoS issues

- well known, unfortunate side effects of authentication systems.

9. I note that Veneklasė fails no better in dealing with the problem of DoS attacks. There is no disclosure in Veneklasė that would lessen the chances of a DoS attack. The use of Veneklasė's two passwords does not lessen the chance of a DoS attack because a hacker would still trigger DoS through repeated invalid access attempts, thereby overwhelming the system and preventing authorized users from gaining access, i.e., a DoS attack.

10. Finally, Patent Owner asserts that Veneklasė's teaching of an algorithm for additional security is not an explicit teaching, suggestion, or motivation for combining Veneklasė with Jonsson's teachings. I disagree. A POSITA would have understood that Veneklasė's specific teaching of using algorithms to enhance security would have provided a suggestion to employ other algorithms related to security in order to further Veneklasė's explicitly stated goal to "ensure that only authorized users gain access to a computer system." EX1005, 3:31-33. Patent Owner's rationale is akin to saying that a POSITA would not be motivated to modify a security system that utilizes one type of lock, e.g., a padlock, by using another type of lock, e.g., a combination lock.

B. Limitation [5.4] "a communication module configured to transmit the token to the personal communication device through the cell phone network;"

11. I note that this limitation is directed to the communication module, but

Patent Owner appears to attack the method of identifying a user's device. In particular, Patent Owner argues that the inability to look up a phone number somehow negates the combination. I do not agree with this assertion as there would not be a requirement to look up a phone number in the combination with Jonsson. In particular, Jonsson discloses:

A user initiates a service access through terminal 22 by transmitting the request over a service access network 24 to a service node 26. The service node 26 does not immediately initiate the services offered. Rather, it generates a challenge code or causes a challenge code to be generated in an authentication center 30. The challenge code is sent over an authentication challenge network 28 to the personal unit.

Ex. 1006, 9:2–8; also 10:13–27, Fig. 3. Thus, in the combination, there is no need to look up a phone number in the combination.

12. Patent Owner also reiterates its arguments regarding DoS attacks. For the same reasons I discuss above, a POSITA would not have understood that Veneklas was any more effective at avoiding or stopping DoS attacks.

C. Limitation [5.5] “an authentication module configured to receive the password from the user through a secure computer network,”

13. Patent Owner states that because Veneklas's system uses “off the shelf” and readily available components, that it would not be capable of performing the software implemented methods of Jonsson. This is contradicted by

the express disclosure of Jonnson that “the capacity for performing the necessary calculations exists in conventional cellular telephones and personal communication units, allowing the present invention to be implemented through software.”

EX1006, 7:21-31. Patent Owner attempts to distinguish from this clear teaching by citing the preceding sentence describing a preferred embodiment where the personal unit is a separate unit. 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. Further, Veneklasé already discloses that its pager unit executes algorithms. EX1005, 9:26-10:11. Thus, a POSITA would have understood that the pager of Veneklasé was capable of performing the algorithms of Jonsson.

D. Limitation [5.6] “wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account, such that said account is not accessible through any password via the secure computer network,”

14. Patent Owner makes four separate arguments with respect to this limitation. I address each below.

15. First, Patent Owner alleges that Veneklasé does not activate access in response to the creation of the password. As an initial matter, the claim does not include the language “creation of” or any variation thereof. Thus, my previous declaration demonstrated how Veneklasé activates access to the account (e.g.,

allows access) in response to the entry of the password. I am informed that a district court has interpreted 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.” While I disagree with this interpretation injecting extraneous words into the claim, it does not change the fact that the combination of Veneklase and Jonnson discloses this limitation even under the court’s interpretation.

16. Patent Owner is taking the position that “activates access” is something that happens before access is granted. However, this is a gratuitous point, as access to the account has to be activated in order for the created password to work, i.e, the account is accessed. In other words, the account cannot be used when the account is deactivated. I am not aware of any system that does not “activate access” to the account when generating a new password as this would undermine the purpose of generating a new password, i.e., accessing an account.

17. 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 a response. As such, Jonsson teaches activating access to the account in response to

the creation of the password under the district court's interpretation.

18. In addition, Jonsson discloses that “the challenge code and the response is unique for each transaction.” EX1006, 3:16-18. A POSITA would have understood this disclosure to mean 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., password) because prior response codes would not have worked. In other words, 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.

19. Second, Patent Owner alleges that the claimed predetermined amount of time is the timeframe between activation and deactivation of the account. However, Patent Owner mistakes the “predetermined amount of time after activating the account” to mean the entire period after account access is activated. Rather, a POSITA would have understood that this claim limitation simply means any predetermined period *after* activation. 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.

20. 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.” 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. However, as discussed above, 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. 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. Thus, the “authentication module” (i.e., “code compare module 416” in the “host computer”) is responsible for account deactivation.

21. Finally, Patent Owner alleges that “the predetermined period of time” varies by when the user decides to send back the response code. This completely ignores Veneklasé’s teaching that the password must be “received within a predetermined period of time.” As explained above, the combination of Veneklasé

and Jonsson meets the deactivation limitation. EX1005, 8:40-49.

III. GROUND 2

22. Patent Owner makes several arguments in an attempt to distinguish from the combination of Kew and Sormunen. Again, Patent Owner's analysis fails to understand and apply the teachings of the cited references from the perspective of a POSITA. Patent Owner's arguments are limited to limitations [5.3], [5.6], and [1.2], which I address below.

A. Limitation [5.3]- the "passcode"

23. In my previous declaration, I identified the User ID/IdentityCode as the "passcode" limitation. 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. 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.

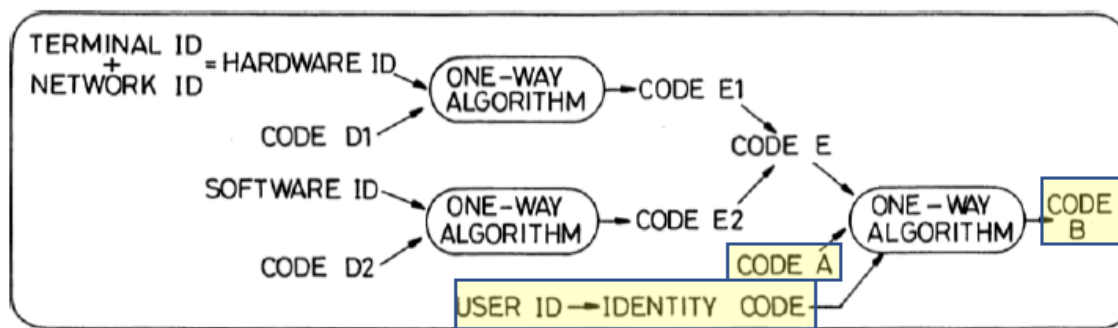
When the user seeks access to the host system 1 via the terminal 2 , **he enters his user identification code**. This code may take any suitable form, for example his actual name or preferably a more secure code such as a PIN. The security server 5 includes a database of all authorised users and their 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.

24. 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. In particular, I cited both the user identity code (user ID) and the corresponding identity code to demonstrate that a Code B (e.g., password) is generated based on: 1) Code A (e.g., token) and 2) the user ID and the “corresponding identity code” (e.g., passcode) . 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. 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.

25. This process is illustrated in Ex. 1007, Fig. 2, which I previously cited:



26. As shown above, and explained in Kew, 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 appreciate 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. 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 because that is what is used to identify the algorithm used by the receiver.

27. Patent Owner also asserts that “identity code” would not be known to the user. However, Patent Owner’s arguments relate to the programming of the receiver and do not support a conclusion that the identity code would not be known to the user. The programming of the receiver and storage of the identify code in the EPROM is not relevant to whether the user has knowledge of the identity code. Also, the reprogramming of the EPROM using ultraviolet light is similarly irrelevant to whether the user knows the identity code. EPROM means “erasable programmable *read*-only memory.” This meaning says nothing about who can read the memory, just that it cannot be written to (without having been first erased using ultraviolet light) . Nothing about the design of the EPROM storage of the “identity code” prevents the user from knowing its contents or value. Indeed, as the name indicates, EPROM is necessarily readable.

28. Kew does not say that the identity code is unknown to the user, and Patent Owner does not give any reason why the identity code would be secret or hidden from the user. Rather, a POSITA would have understood that it would be practical for the user 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 receiver would be useless and the user would not be able to access the system. As noted by Patent Owner, reprogramming the EPROM

requires exposing the chip to ultraviolet light, which is a process that would be impractical for a layperson user. Further, as Patent Owner indicates, changing the identity code would also require updating the database to also include the new identity code. 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. 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.

29. I also note that there is no disclosure in Kew that prevents the user identification code from being the same as the identity code. In fact, Claim 1 of Kew supports such a situation, as the “input user identification code” is performing the same function as the identity code of identifying the transformation algorithm to generate Code B.

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

Thus, claim 1 of Kew supports the user ID as the same as the identity code.

B. Limitation [5.6] “activates access to the account in response to the password”

30. In my previous declaration, I demonstrated how Kew discloses that access to the account is activated in response to the password, as claimed. I am informed that a district court has interpreted 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.” While I disagree with this interpretation injecting extraneous words into the claim, it does not change the fact that Kew discloses this limitation even under the court’s interpretation. In particular, it appears that Patent Owner is taking the position that “activates access” is something that happens before access is granted. However, this is a gratuitous point, as access to the account has to be activated in order for the created password to work, i.e., access is granted. In other words, the account cannot be used when the account is deactivated. I am not aware of any system that does not “activate access” to the account when generating a new password as this would undermine the purpose of generating a new password, i.e., accessing an account.

31. Kew discloses “activates access” under Patent Owner’s interpretation because the creation of the new password (Code B) is activating access to the

account. Kew sends Code A to the receiver so that it can be transformed into Code C. EX1007, 2:27-34. 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. *Id.* Thus, a POSITA would have understood that Kew's generation of Code B is "activating access" to the account.

C. Limitation [5.6] "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"

32. Patent Owner alleges that Kew does not disclose that the "security server 5" deactivates the account. Response at 53. In particular, Patent Owner alleges that "account access remains active indefinitely after Code A has been transmitted." This is another instance of not understanding the disclosure of Kew from the perspective of a POSITA. As I point out in my previous declaration at paragraph 150, 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 which I discuss in paragraph 49 of my previous declaration.

33. The concept of the "timeliness" or "lifetime" of information or its "freshness" was well known for cryptographic keys as well as authentication systems well before the '658 Patent's priority date. The concept of "aging" of

cryptographic keys has been known for more than a half century with encryption keys swapped out after predefined “crypto periods,” often in a 24 hour period (e.g., see Gen. Charles H. Myer, “Viet Nam Studies – Division-Level Communications 1962-1973,” Department of the Army, CMH PUB 90-11, 1982, EX1021, p. 71) . After the crypto period when a cryptographic key was valid, attempts to access a system using a “stale” cryptographic key would fail because the information was now encrypted using a different key, rendering the information useless to the user without a current key. The concept of “freshness” of authentication information is also well known, for instance, as described by Stubblebine (S. G. Stubblebine, "Recent-secure authentication: enforcing revocation in distributed systems," *Proceedings 1995 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 1995, pp. 224-235, doi: 10.1109/SECPRI.1995.398935) , EX1022. As Stubblebine describes, revocation of access is needed for several reasons, perhaps because of compromise, change of affiliation, or cessation of an entity’s operation, among other reasons. Further, specific mechanisms to ensure the “freshness” or “timeliness” of cryptographic keys or challenge-response values has been well known before the ’658 patent, e.g. Boyd (C. Boyd, "A class of flexible and efficient key management protocols," *Proceedings 9th IEEE Computer Security Foundations Workshop*, Kenmare, Ireland, 1996, pp. 2-8, doi: 10.1109/CSFW.1996.503685, EX1023) . It has been commonly known in the

design of secure systems long before the filing of the '658 patent that, on general principles, the longer an authentication parameter or cryptographic key is in use and more information becomes dependent on its security, the greater the chance of compromise of that information, necessitating frequent updates, depending on the criticality of the information being protected. Accordingly, the concept of time-based access was well established before the '658 Patent.

34. Kew teaches time-based access. 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 (time-bound access), as allowing Code C to be valid indefinitely, as Patent Owner suggests, would be contrary to time-based access and compromise security as was well-known prior to the '658 Patent's priority date of March 6, 2000. 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 as of March 6, 2000. 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.

35. A POSITA would have understood that the “predetermined length of time” was known by both the security server 5 and the receiver. In particular, Kew discloses 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. 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. Otherwise, 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. Such a scenario would be counter to the goal of achieving time-bound access for the reasons I provide above.

36. Further, I note that the disclosure of Kew is clear in that the security server “prompts” entry of the “transformed Code C **displayed by the receiver unit 6.**” EX1006, 9;6-7. If the account access was not deactivated when the display was

no longer displaying Code C, Kew would have simply disclosed entry of “transformed Code C” and not specified that it must be “displayed by the receiver unit 6.” 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. As noted by Patent Owner, 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. Accordingly, a POSITA would have understood that the security server of Kew must, at a minimum, 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.

37. Kew also demonstrates time-bound access through limiting the ability of the receiver to generate Code C. 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.” Patent Owner 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. Patent Owner’s interpretation of Kew is based on the faulty premise that Kew’s codes are “active indefinitely” and ignores that this disclosure relates to the ability to transform Code A to Code C, and not merely to the ability to display Code C.

However, this is not how Kew functions, and not how a POSITA would have understood Kew's time-bound access to add security.

38. Kew's disclosure relates to permitting the algorithm to transform Code A to Code C for a limited time once it is received by the receiver. This is consistent with the known time-based security solutions as of the priority date of the '658 patent. 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. 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. 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."

39. 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.

In sum, Kew discloses two methods for ensuring 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. The second method enables the receiver to transform Code A to Code C for “predetermined period.” A POSITA would have understood that this was accomplished by limiting the lifetime of Code A to the “predetermined period.”

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

40. Patent Owner alleges that the proposed modification to Kew with the disclosure of Sormunen would somehow require the entry of Kew’s user ID twice. I disagree and a 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. 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. 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 of the user ID on the receiver. EX1007, 9:27-31.

41. I note 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. 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. Thus, even under Patent Owner’s interpretation requiring a double transmission of the user ID, the system of Kew is secure against unauthorized access.

IV. CONCLUSION

42. In signing this declaration, I recognize that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross examination in the case and that cross examination will take place

within the United States. If cross examination is required of me, I will appear for cross examination within the United States during the time allotted for cross examination.

43. I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct, and that all statements made of my own knowledge are true and that all statements made on information and belief are believed to be true. I understand that willful false statements are punishable by fine or imprisonment or both. *See* 18 U.S.C. § 1001.

Date: January 9, 2024

Respectfully submitted,



Bruce McNair