

**UNITED STATES PATENT AND TRADEMARK OFFICE**

---

**BEFORE THE PATENT TRIAL AND APPEAL BOARD**

---

AMAZON.COM, INC.,

Petitioner,

v.

DYNAPASS IP HOLDINGS LLC,

Patent Owner.

---

Case No. IPR2024-00283

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

**DECLARATION OF DR. JON B. WEISSMAN IN SUPPORT OF PETITION  
FOR *INTER PARTES* REVIEW OF  
CLAIMS 2 AND 7 OF U.S. PATENT NO. 6,993,658**

## TABLE OF CONTENTS

|                                                                                                                                                                                                                                                                           | Page |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| I. INTRODUCTION & QUALIFICATIONS .....                                                                                                                                                                                                                                    | 1    |
| A. Engagement .....                                                                                                                                                                                                                                                       | 1    |
| B. Qualifications .....                                                                                                                                                                                                                                                   | 2    |
| II. MATERIALS REVIEWED .....                                                                                                                                                                                                                                              | 5    |
| III. DESCRIPTION OF THE RELEVANT TIMEFRAME, THE<br>RELEVANT FIELD, AND A PERSON OF ORDINARY SKILL IN<br>THE ART.....                                                                                                                                                      | 6    |
| MY UNDERSTANDING OF CERTAIN LEGAL STANDARDS .....                                                                                                                                                                                                                         | 8    |
| IV. SUMMARY OF MY OPINIONS .....                                                                                                                                                                                                                                          | 11   |
| V. CLAIM CONSTRUCTION .....                                                                                                                                                                                                                                               | 13   |
| VI. BACKGROUND .....                                                                                                                                                                                                                                                      | 14   |
| A. The '658 Patent .....                                                                                                                                                                                                                                                  | 14   |
| B. Cited References.....                                                                                                                                                                                                                                                  | 18   |
| 1. Veneklas (Ex.1005).....                                                                                                                                                                                                                                                | 19   |
| 2. Jonsson (Ex.1006).....                                                                                                                                                                                                                                                 | 20   |
| 3. Sormunen (Ex.1007) .....                                                                                                                                                                                                                                               | 22   |
| 4. Kaufman (Ex.1008).....                                                                                                                                                                                                                                                 | 23   |
| 5. Kew (Ex.1009).....                                                                                                                                                                                                                                                     | 24   |
| VII. MY OPINIONS AS TO <i>VENEKLASE</i> , <i>JONSSON</i> , AND<br><i>SORMUNEN</i> AND THE OBVIOUSNESS OF CLAIM 7.....                                                                                                                                                     | 26   |
| A. Claim 5 .....                                                                                                                                                                                                                                                          | 27   |
| 1. Claim 5[pre]— “A user authentication system<br>comprising:” .....                                                                                                                                                                                                      | 27   |
| 2. Claim 5[a]— “a computer processor;” .....                                                                                                                                                                                                                              | 28   |
| 3. Claim 5[b]— “a user database configured to associate a<br>user with a personal communication device possessed by<br>the user, said personal communication device configured<br>to communicate over a cell phone network with the user<br>authentication system;” ..... | 30   |

**TABLE OF CONTENTS**  
(continued)

|                                                                                                                                                                                                                                                                                                                                                                                   | <b>Page</b> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 4. Claim 5[c]— “a control module executed on the computer processor configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a password associated with the user to be the new password;” .....                     | 35          |
| 5. Claim 5[d]— “a communication module configured to transmit the token to the personal communication device through the cell phone network; and” .....                                                                                                                                                                                                                           | 40          |
| 6. Claim 5[e]— “an authentication module configured to receive the password from the user through a secure computer network, said secure computer network being different from the cell phone network,” .....                                                                                                                                                                     | 42          |
| 7. Claim 5[f]— “wherein the user has an account on the secure computer network, wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account, such that said account is not accessible through any password via a secure computer network.” ..... | 46          |
| B. A POSITA Would Have Been Motivated to Combine <i>Veneklase</i> and <i>Jonsson</i> .....                                                                                                                                                                                                                                                                                        | 51          |
| C. Claim 6 .....                                                                                                                                                                                                                                                                                                                                                                  | 56          |
| D. Claim 7 .....                                                                                                                                                                                                                                                                                                                                                                  | 58          |
| E. A POSITA Would Have Been Motivated to Combine <i>Veneklase</i> , <i>Jonsson</i> , and <i>Sormunen</i> .....                                                                                                                                                                                                                                                                    | 61          |
| VIII. MY OPINIONS AS TO CLAIM 2 IN CONSIDERATION OF <i>VENEKLASE</i> IN VIEW OF <i>JONSSON</i> , <i>SORMUNEN</i> , AND <i>KAUFMAN</i> .....                                                                                                                                                                                                                                       | 66          |
| A. Claim 1 .....                                                                                                                                                                                                                                                                                                                                                                  | 66          |

**TABLE OF CONTENTS**  
(continued)

|                                                                                                                                      | <b>Page</b> |
|--------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 1[b]— “receiving a request from the user for a token via the personal communication device, over the second network;” .....          | 67          |
| B. Claim 2 .....                                                                                                                     | 69          |
| C. A POSITA Would Have Been Motivated to Combine <i>Veneklase, Jonsson, Sormunen, and Kaufman</i> .....                              | 72          |
| IX. MY OPINIONS AS TO CLAIM 7 IN CONSIDERATION OF <i>KEW</i> IN VIEW OF <i>SORMUNEN</i> .....                                        | 76          |
| A. My Opinions as to Aspects of Claim 7 that are Inherited from Claim 5 .....                                                        | 76          |
| 1. 5[pre] .....                                                                                                                      | 76          |
| 2. 5[a] .....                                                                                                                        | 77          |
| 3. 5[b] .....                                                                                                                        | 79          |
| 4. 5[c] .....                                                                                                                        | 83          |
| 5. 5[d] .....                                                                                                                        | 86          |
| 6. 5[e] .....                                                                                                                        | 88          |
| 7. 5[f] .....                                                                                                                        | 90          |
| B. Claim 6 .....                                                                                                                     | 94          |
| C. Claim 7 .....                                                                                                                     | 95          |
| D. A POSITA Would Have Been Motivated to Combine <i>Kew</i> and <i>Sormunen</i> .....                                                | 97          |
| X. MY OPINIONS AS TO CLAIM 2 IN CONSIDERATION OF <i>KEW</i> IN VIEW OF <i>SORMUNEN</i> AND <i>KAUFMAN</i> .....                      | 102         |
| A. Claim 1 .....                                                                                                                     | 102         |
| 1. Claim 1[b]— “receiving a request from the user for a token via the personal communication device, over the second network;” ..... | 103         |
| B. Claim 2 .....                                                                                                                     | 104         |

**TABLE OF CONTENTS**  
(continued)

|                                                                                                             | <b>Page</b> |
|-------------------------------------------------------------------------------------------------------------|-------------|
| C. A POSITA Would Have Been Motivated to Combine <i>Kew</i> ,<br><i>Sormunen</i> , and <i>Kaufman</i> ..... | 107         |
| XI. CONCLUSION.....                                                                                         | 111         |

## PETITIONER'S EXHIBIT LIST

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

I, Jon B. Weissman, hereby declare as follows:

**I. INTRODUCTION & QUALIFICATIONS**

**A. Engagement**

1. I have been retained on behalf of Amazon.com, Inc. (“Amazon” or “Petitioner”) in connection with the above-captioned petition for *Inter Partes* Review (“IPR”) of claims 2 and 7 of U.S. Patent No. 6,993,658 (the “’658 Patent” or “Ex. 1001”). I understand the ’658 Patent is currently assigned to Dynapass IP Holdings LLC (“Patent Owner”).

2. Petitioner has asked me to offer opinions regarding the ’658 Patent, including whether claims 2 and 7 (which I may refer to subsequently as the “Challenged Claims”) are valid in view of certain prior art. This declaration sets forth the opinions I have reached to date regarding these matters.

3. I am being compensated by Petitioner at my standard hourly consulting rate of \$700 for my time spent on this matter. My compensation is not contingent on my findings or the outcome of this proceeding. I have no financial interest in the ’658 Patent, Petitioner, Patent Owner, or the outcome of this matter.

4. This declaration briefly outlines my background and qualifications, describes the technology at issue and background of the art, identifies materials I reviewed to prepare this declaration, and sets forth my understanding of the patent claims and my analysis regarding unpatentability of the Challenged claims in view

of the prior art discussed herein. I reserve the right to supplement my opinions in the future, to clarify responses where appropriate, and to take into account new information as it becomes available to me.

**B. Qualifications**

5. My academic and professional background is in computer science, specifically in the areas of data storage, file systems, backup/restore, distributed computing, cloud computing, and developing and testing large-scale software systems. I am a leading researcher and educator in these areas. My career includes over 25 years of experience in industry and academia in building, testing, and analyzing, such software systems. As a systems researcher, I have built practical systems that have applications in a wide variety of settings across diverse types of distributed and parallel systems. A list of my prior testimony and cases in which I supported various topics, including security methods and two-factor authentication, is included in my *curriculum vitae* (“CV”), which is provided as Ex.1003.

6. I am a Full Professor of Computer Science at the University of Minnesota. I received my B.S. in Applied Mathematics and Computer Science from Carnegie-Mellon in 1984, and my M.S. and Ph.D. in Computer Science from the University of Virginia, with my M.S. earned in 1989 and my Ph.D. in 1995.

7. In addition to my professorship, I lead the University of Minnesota’s Distributed Computing Systems Group. The Distributed Computing Systems

Group is focused on research into distributed and mobile systems, cloud computing, and high-performance computing. The Distributed Computing Systems Group also investigates cross-cutting topics including storage, networking, operating systems/middleware, security, and applications.

8. As part of my work leading the Distributed Computing Systems Group, I designed a security system for our mobile Internet of Things (“IoT”) platform.

9. I have extensive experience with developing technologies and techniques to improve security in backup/restore technologies. For example, as an investigator for the University of Minnesota Center for Intelligent Storage (CRIS) for over a decade, I was involved in Massive Array of Idle Disks (MAID) for archival storage. CRIS brought together both industry and academic partners to solve emerging storage problems in file and storage systems by exploring and developing new technologies and techniques to improve the usability, scalability, security, reliability, efficiency, and performance of storage systems for several use cases including backup.

10. I have published over 100 peer-reviewed technical articles, including some awarded or nominated for Best Paper at highly competitive international conferences. Many of my published papers relate to security topics, including this small sample (and many more listed on my CV):

- “SQuBA: Social Quorum Based Access Control for Open IoT Environments,” Yixuan Wang, Abhishek Chandra, Jon Weissman, IEEE Edge 2023, best student paper awardee;
- “A Security-enabled Grid System for MINDS Distributed Data Mining,” Jinoh Kim, Seonho Kim, Jon B. Weissman, Journal of Grid Computing, 2014;
- “Adaptive middleware supporting scalable performance for high-end network services,” Byoung-Dai Lee, Jon B. Weissman, Young-Kwang Nam, Journal of Network and Computer Applications, 2009;
- “DDDAS/ITR: A Data Mining and Exploration Middleware for Grid and Distributed Computing,” Jon B. Weissman, Vipin Kumar, Varun Chandola, Eric Eilertson, Levent Ertoz, Gyorgy Simon, Seonho Kim, Jinoh Kim, Workshop on Dynamic Data Driven Application Systems – DDDAS 2007, Beijing, China, 2007;
- “Reputation-Based Scheduling on Unreliable Distributed Infrastructures,” Jason Sonnek, Mukesh Nathan, Abhishek Chandra, Jon Weissman, Proceedings of the 26<sup>th</sup> International Conference on Distributed Computing Systems (ICDCS ’06), Lisboa, Portugal, July 2006;

- “A Quantitative Comparison of Reputation Systems in the Grid,”  
Jason D. Sonnek, Jon B. Weissman, 6<sup>th</sup> IEEE/ACM International  
Workshop on Grid Computing, 2005.

11. I routinely teach classes in operating systems at both the undergraduate and graduate level in which I teach students about security methods, including two-factor authentication. A list of courses that I teach as a Professor of Computer Science is included in my CV, which is included as Exhibit 1003.

12. I have also served on the boards of several flagship journals, including IEEE Transactions on Parallel and Distributed Systems and IEEE Transactions on Computers. I am the steering committee chair of the ACM International Symposium on High Performance Parallel and Distributed Systems, the flagship conference in my area. And I serve as an investigator for both the Center for Research in Intelligent Storage (sponsored by the National Science Foundation) and the Digital Technology Center.

## **II. MATERIALS REVIEWED**

13. My opinions are based on a review of the materials of record in this proceeding, including the '658 Patent and its prosecution history, and each of the documents listed in the Exhibit List above and any other materials cited herein. I understand that other third parties, including Unified Patents, have filed *inter partes* review petitions on certain claims of the '658 Patent. Ex.1012 (Unified

Amazon.com – Ex.1002

Petition); Ex.1013 (Unified Institution Decision). I understand that the Unified IPR did not challenge claims 2 or 7, which are the claims that are challenged here. I further understand that my opinions rely on some of the same references and arguments as asserted in the Unified IPR Petition.

14. In reaching my opinions, I have also relied upon my general knowledge and experience in the field and also considered the viewpoint of a person having ordinary skill in the art (“POSITA”) at the time of the filing date of the ’658 Patent, *i.e.*, March 6, 2000. As explained below, I am very familiar with the level of skill of a POSITA regarding the relevant technology at issue as of that time.

### **III. DESCRIPTION OF THE RELEVANT TIMEFRAME, THE RELEVANT FIELD, AND A PERSON OF ORDINARY SKILL IN THE ART**

15. All of the opinions that I provide herein are provided through the lens of a POSITA during the relevant time period. I understand that the ’658 Patent was filed on March 6, 2000. For the purposes of my analysis, and in the absence of any information to the contrary, I have used the March 6, 2000 date as the relevant priority date (which I may refer to for simplicity as the “Priority Date”) for my analysis of the prior art.

16. I considered several factors to determine the skill level of a POSITA of the ’658 Patent as of the Priority Date, including the types of problems

encountered in the art, solutions to those problems, the pace of innovation in the field, the sophistication of the technology, and the education level of active workers in the field.

17. A POSITA of the '658 Patent would have had at least (1) an undergraduate degree in electrical and computer engineering or a closely related field; and (2) two or more years of experience in security. Additional advanced educational degrees could substitute for some years of experience, and, likewise, additional industry experience could substitute for educational degrees as well.

18. In addition, a POSITA would have been familiar with the principles that the '658 Patent admits as being part of the general knowledge of the art, including, but not limited to, (A) operating systems controlling local area networks of workstations within a business or institution typically require submitting a user ID and password combination before allowing access to a workstation; and (B) two-factor authentication processes, such as that provided by the SecurID product, distributed by RSA Security Inc., where the first factor is a user passcode/personal identification number and the second factor is a SecurID card possessed by the user. The SecurID card generates and displays unpredictable, one-time-only access codes that automatically change every 60 seconds and the user supplies the displayed code upon logging into a system. The system has a corresponding “code generator” that verifies possession of the SecurID card. Ex.1001, 1:15-53.

19. Unless noted otherwise, when I state that something would be known or understood by one skilled in the art, or a skilled artisan, or a POSITA, I am referring to a person with the level of education and experience that I outlined above in the time period on or before the Priority Date.

### **MY UNDERSTANDING OF CERTAIN LEGAL STANDARDS**

20. In formulating my opinions, I have been instructed to apply certain legal standards. I am not a lawyer and have not been asked to offer my opinion on the law. Counsel has informed me of the applicable legal standards, as set forth in the following sections. The following sections summarize the law as I have been instructed to apply it in formulating and rendering my opinions found later in this declaration. I understand that, in an *Inter Partes* Review proceeding, patent claims may be deemed unpatentable if it is shown that they are obvious in view of the prior art. I understand that prior art in an *Inter Partes* Review is limited to patents or printed publications that qualify as prior art.

21. I understand that when considering the scope of the claims of a patent that the patent claim terms should generally be given the ordinary meaning that the terms would have to a POSITA.

22. I understand that the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the term appears, but in the context of the entire patent, including the specification. I

further understand that the principal considerations regarding the scope and meaning of the claims are the plain language of the claim (including the surrounding claim language and context), the patent specification, and the prosecution history. I understand that while a claim is to be read in light of the specification, one must generally avoid importing limitations into the claim from the specification. I am also informed that the prosecution history can often inform the meaning of the claim by demonstrating how the inventor understood the invention and whether the inventor limited the invention in the course of prosecution, making the claim scope narrower than it would otherwise be. I applied these understandings when considering the scope and meaning of the claims of the '658 Patent.

23. I understand that a claim is unpatentable if it would have been obvious. Obviousness of a claim requires that the claim would have been obvious from the perspective of a POSITA at the time the alleged invention was made. I understand that a claim could have been obvious from a single prior art reference or from a combination of two or more prior art references.

24. I understand that an obviousness analysis requires an understanding of the scope and content of the prior art, any differences between the alleged invention and the prior art, and the level of ordinary skill in evaluating the pertinent art.

25. I further understand that a claim would have been obvious if it unites old elements with no change to their respective functions, or merely substitutes one element for another known in the field, and that combination yields predictable results. While it may be helpful to identify a reason for this combination, I understand that there is no strict requirement of finding an express teaching, suggestion, or motivation to combine within the references. When a product is available, design incentives and other market forces can prompt variations of it, either in the same field or different one. If a POSITA can implement a predictable variation, obviousness likely bars its patentability. For the same reason, if a technique has been used to improve one device and a POSITA would recognize that it would improve similar devices in the same way, using the technique would have been obvious. I understand that a claim would have been obvious if common sense directs one to combine multiple prior art references or add missing features to reproduce the alleged invention recited in the claims.

26. I understand that in considering obviousness, it is important not to determine obviousness using the benefit of hindsight derived from the descriptions found in the patent being considered.

27. I further understand that certain factors may support or rebut the obviousness of a claim. I understand that such secondary considerations include, among other things, commercial success of the patented invention, skepticism of

those having ordinary skill in the art at the time of invention, unexpected results of the invention, any long-felt but unsolved need in the art that was satisfied by the alleged invention, the failure of others to make the alleged invention, praise of the alleged invention by those having ordinary skill in the art, and copying of the alleged invention by others in the field. I understand that there must be a nexus—a connection—between any such secondary considerations and the alleged invention.

28. I also understand that contemporaneous and independent invention by others is a secondary consideration tending to show obviousness. I am not aware of any allegations by the named inventors of the '658 Patent or any assignee of the '658 Patent that any secondary considerations tend to rebut the obviousness of any challenged claim of the '658 Patent.

29. I understand that Petitioner has the burden of proving unpatentability by a preponderance of evidence, which means that the claims are more likely than not unpatentable.

The analysis in this declaration is in accordance with the above-stated legal principles.

#### **IV. SUMMARY OF MY OPINIONS**

41. Having reviewed the '658 Patent and the prior art references in the Exhibit List above, I have formed the following opinions:

- The combination of *Veneklase* in view of *Jonsson* and *Sormunen* discloses all limitations of claim 7 and the claim is rendered obvious by the combination;
- The combination of *Veneklase* in view of *Jonsson*, *Sormunen*, and *Kaufman* disclose all limitations of claim 2 and the claim is rendered obvious by the combination;
- The combination of *Kew* in view of *Sormunen* discloses all limitations of claim 7 and the claim is rendered obvious by the combination; and
- The combination of *Kew* in view of *Sormunen* and *Kaufman* discloses all limitations of claim 2 and the claim is rendered obvious by the combination.

42. A table displaying the grounds of invalidity is shown below:

| Ground | Prior Art                                                                         | Claim |
|--------|-----------------------------------------------------------------------------------|-------|
| 1      | <i>Veneklase</i> in view of <i>Jonsson</i> and <i>Sormunen</i>                    | 7     |
| 2      | <i>Veneklase</i> in view of <i>Jonsson</i> , <i>Sormunen</i> , and <i>Kaufman</i> | 2     |
| 3      | <i>Kew</i> in view of <i>Sormunen</i>                                             | 7     |
| 4      | <i>Kew</i> in view of <i>Sormunen</i> and <i>Kaufman</i>                          | 2     |

43. The reasons for my opinions are discussed in further detail below.

## V. CLAIM CONSTRUCTION

43. I understand that claim construction is a matter of law and that judges construe claims terms in patents. Here, I have been advised that Magistrate Judge Payne did just that in the *JPMorgan* case by recently construing the following terms:

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

Ex. 1011, 16.

44. I have been advised that Judge Payne's construction of the "activates access..." limitation was based on Patent Owner's disclaimer in the BofA and Unified IPRs (Ex.1011, 10-13), which was found to apply only to claim 5. I understand that Judge Payne found that there was no disclaimer for the "activating access..." limitation in claim 1 and afforded that phrase its plain-and-ordinary meaning.

45. I have been instructed to apply Judge Payne’s constructions in my analysis and was also instructed that all other terms should be given their plain meaning, which is how I have interpreted the other terms.

## **VI. BACKGROUND**

### **A. The ’658 Patent**

46. A POSITA would recognize that the ’658 Patent is directed to two-factor authentication. Two-factor authentication uses two factors (e.g., known password and randomly generated code) to verify a user’s identity when logging into a secure system. It is my understanding that the ’658 Patent acknowledges that the named inventors did not invent two-factor authentication. For example, the ’658 Patent admits “[t]he SecurID product, which is distributed by RSA Security Inc.,” already “require[ed] a two-factor authentication process” before the ’658 Patent. Ex.1001, 1:44-53. For the first factor, the SecurID used “a user passcode or personal identification number.” *Id.* For the second factor, the SecurID used a separate handheld card to “generate[] and display[] unpredictable, one-time-only access codes that automatically change every 60 seconds.” *Id.* The user would then use this “one-time-only access code” from the SecurID card to log into the system. *Id.*

47. I understand the ’658 Patent is directed to “the authentication of users of secure systems” and “a system through which user tokens required for user

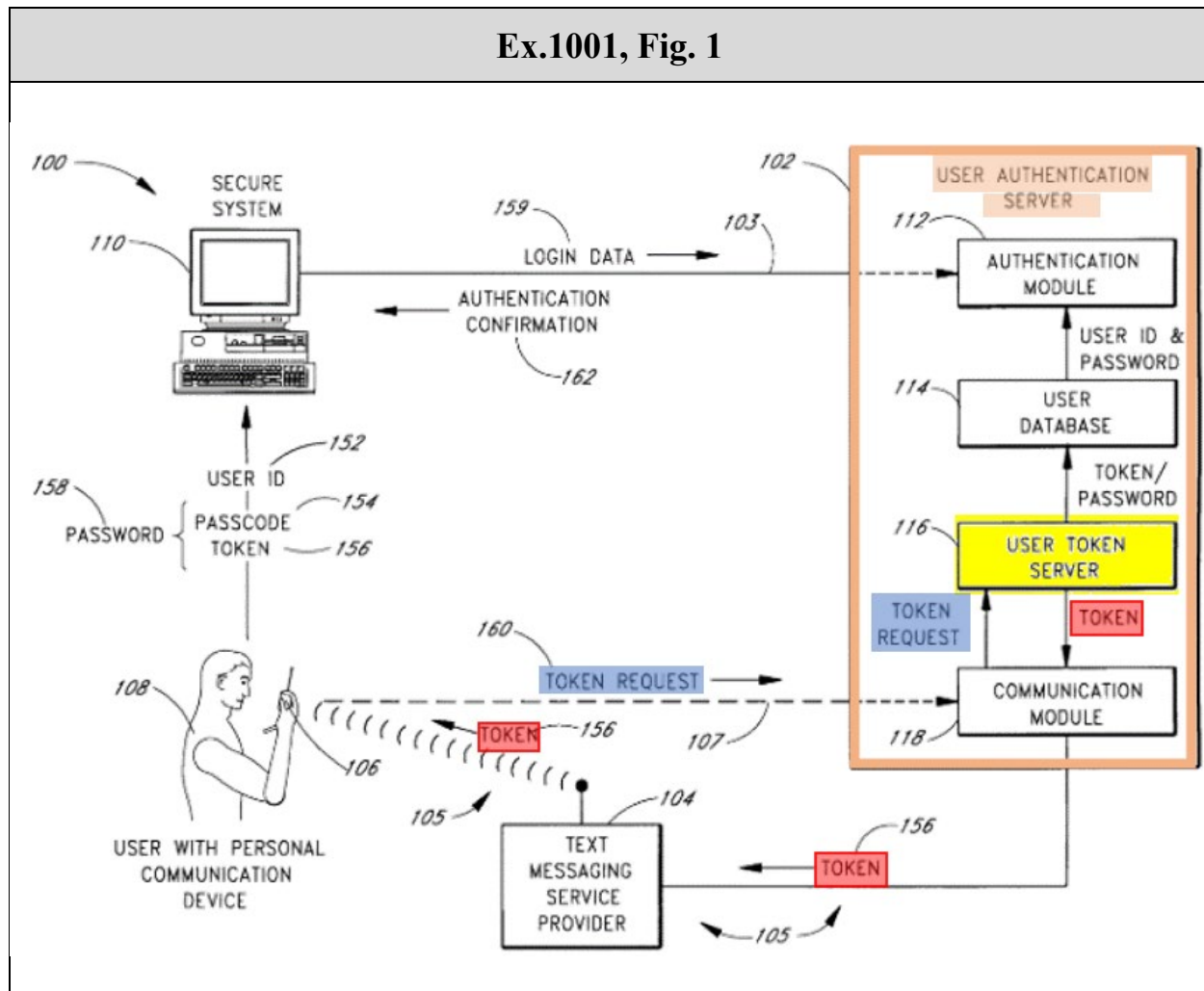
authentication are supplied through personal communication devices such as mobile telephones and pagers.” Ex.1001, 1:7-11. Specifically, the ’658 Patent describes an authentication system in which “access to the system is based upon: nonsecret information known to the user, such as the user ID; secret information known to the user, such as the passcode; and information provided to the user through an object possessed by the user, such as the token.” *Id.*, 2:11-15. I understand the ’658 Patent purports to replace the SecurID card by using “a personal communication device such as a mobile phone or a pager” to obtain the benefits of the SecurID product in “a device that many users already carry.” *Id.*, 1:58-59.

48. As shown in Figure 1 of the ’658 Patent, two annotated versions of which I have reproduced below, in response to a user’s token request 160, user token server 116—which is within the user authentication server—generates a token 156 (e.g., randomly generated code) and creates a new password 158 based on the user’s passcode 154 (e.g., secret password known to user) and the token 156. Ex.1001, 6:59-63, 2:11-15.<sup>1</sup> The token 156 is transmitted to the user’s personal communication device 106 so the user can use it to log in. *Id.*, 7:31-63,

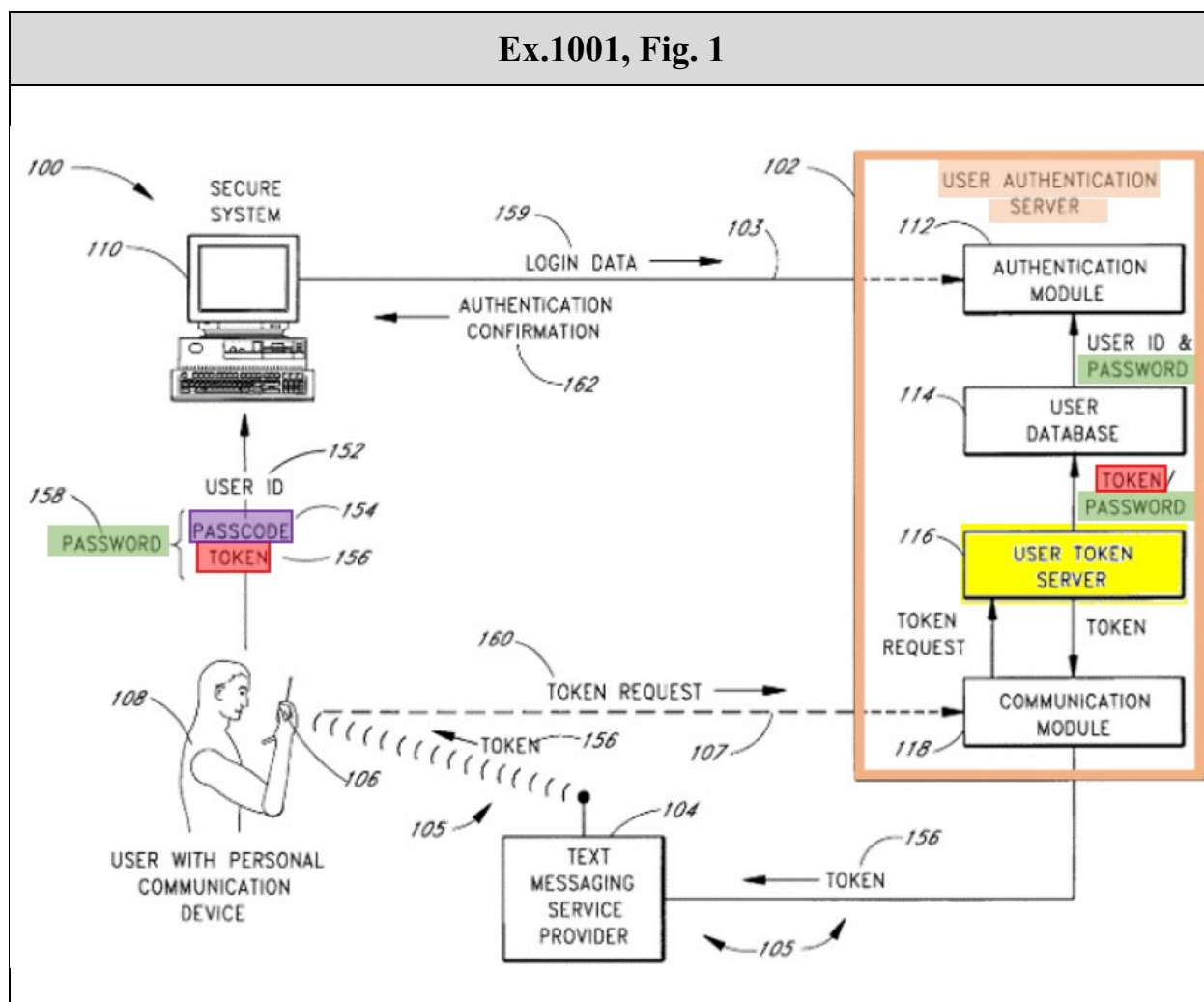
---

<sup>1</sup> Emphasis in textual quotations and annotations/coloring in figures are added throughout, unless otherwise noted.

9:60-64; *see* Ex.1012 (Unified IPR), Paper 1 at 2-4. This is demonstrated in the top annotated image below.



Ex.1001, Fig. 1



49. As shown in the bottom annotated figure reproduced above, after receiving the token, I understand the '658 Patent describes that “the user 108 logs into the secure system 110 using the user ID 152 and the password 158.” Ex.1001, 7:40-45. Once this information is entered into the system by the user, “the authentication server 102 preferably compares the login data to the password 158 (hashed or unhashed) or the passcode 154 and token 156 (hashed or unhashed) corresponding to the user ID 152 stored in the user database 114.” *Id.*, 7:46-63.

“If the token has an expiry time, the token 156 expires,” and “upon expiration of the token 156, the control module 402 deactivates the user account in the user database 114.” *Id.*, 9:60-64.

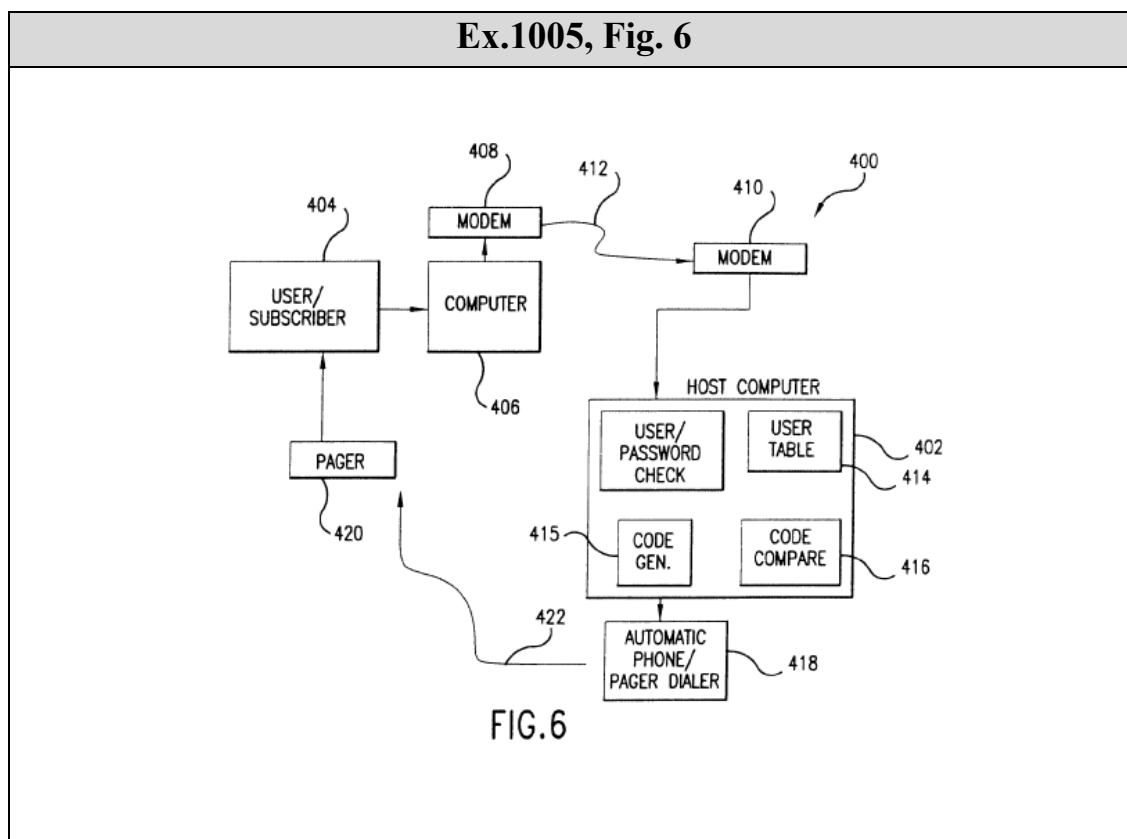
50. With this framework from the ’658 Patent in mind, I would also like to briefly introduce the specific claims on which my opinions are focused, *i.e.*, claims 2 and 7. I note that claim 2 merely requires that “the new password is generated by concatenating the token and the passcode.” In addition, claim 7 merely requires that “the request is transmitted by the user through the personal communication device,” which I note is similarly required by claim 1. *See* Claim 1[b] (“receiving a request from the user for a token via the personal communication device, over the second network”).

## **B. Cited References**

51. I understand that the *Veneklase*, *Jonsson*, *Sormunen*, *Kaufman*, and *Kew* references were previously discussed in the Unified IPR proceedings. Ex.1012, 13-17, 46-50. I also understand that *Sormunen*, while it was cited in the previous IPRs, was not relied on in combination with *Veneklase* and *Jonsson*. I have been informed that each of the cited references relied on qualifies as prior art to the ’658 Patent.

## 1. Veneklas (Ex.1005)

52. A POSITA would have understood that *Veneklas* discloses a system that is “adapted to grant only authorized users access to a computer system.” Ex.1005, 1:5-10; *see id.*, 8:1-15, 7:11-28, 3:50-4:3, claim 5, 8:24-27. In *Veneklas*’s system, as seen in Figure 6 shown below, a user contacts a host computer 402, which “checks the received identification code and cross references the received password code against a pager phone number list resident within the user table 414.” *Id.*, 8:1-5, Fig. 6.



53. I understand that when a match is made, a “code generator...generate[s] a pseudo random number code and passes the received code along with the authorized user’s pager number to the...automatic [phone/pager] dialer 418,” which transmits the code to a user’s device (e.g., pager 420) over a communication channel 422 (e.g., voice line). *Id.*, 8:5-15. I also note that *Veneklase* discloses “utiliz[ing] two distinct communications channels” for sending and receiving the (1) pseudo random code and (2) user’s password. *See id.*, 7:11-28, 3:50-4:3, claim 5.

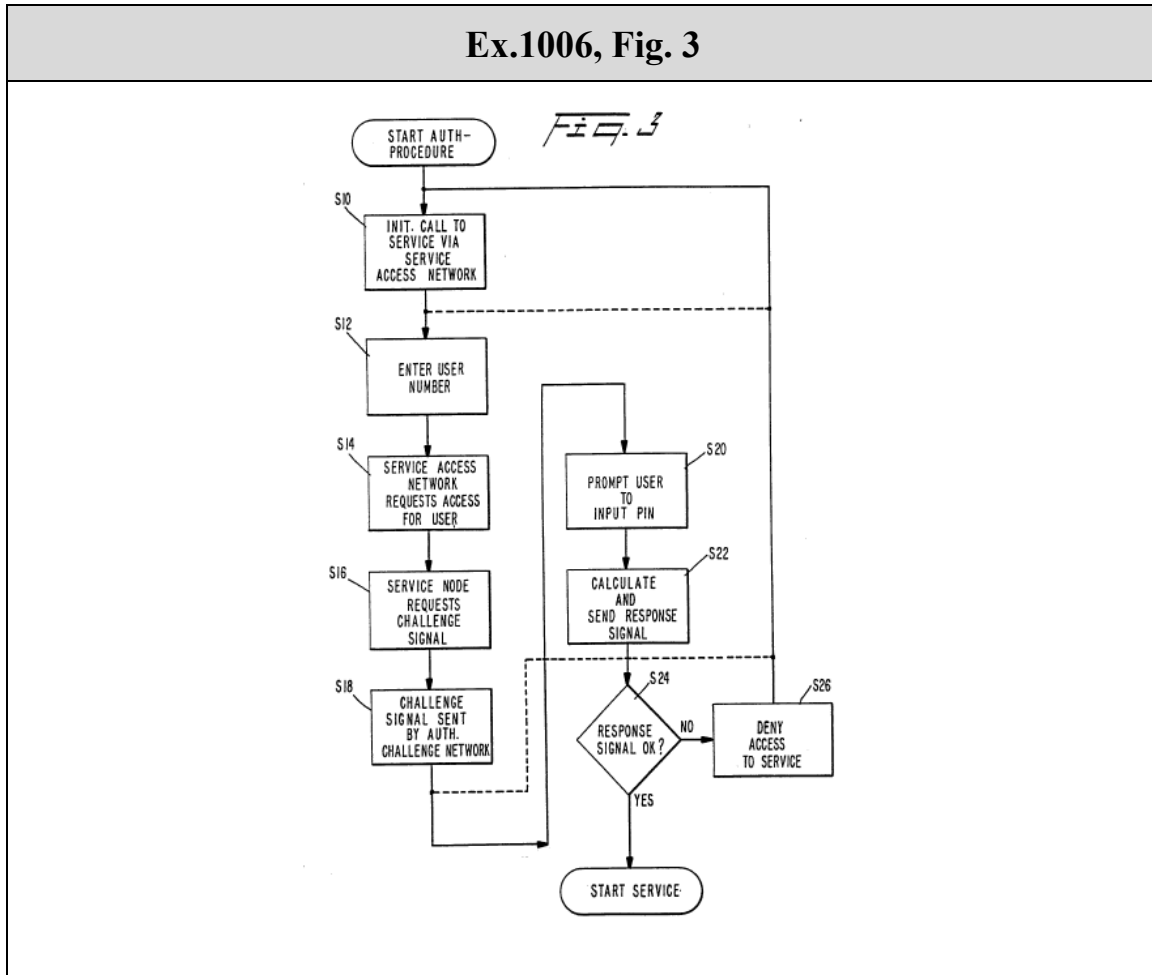
54. I understand the user 404 “enters the code he or she has received from the pager 420...and sends the password or pseudo random code back to computer 402, where it is compared with the software subroutine module denoted as ‘code compare’ 416.” *Id.*, 8:18-24. “If the comparison yields a match, the user 404 is allowed access to computer 402 and/or to a portion of computer 402.” *Id.*, 8:24-27.

## **2. Jonsson (Ex.1006)**

55. A POSITA would understand *Jonsson* discloses a system for providing “[a]uthorization for a user to use a service” via “a modified pager which calculates a unique response code to a transmitted challenge code based on the challenge code, an input personal identification number, and an internal key.”

Ex.1006, Abstract; *see id.*, 10:13-33, 8:12-14, 7:5-10, 9:23-25, 11:4-20. As shown

below in Figure 3 of *Jonsson*, “a user initiates communication to a service node 26 via the service access network 24,” e.g., by “dialing an appropriate telephone number, which may be pre-stored in their personal unit.” *Id.*, 10:13-18, Fig. 3.

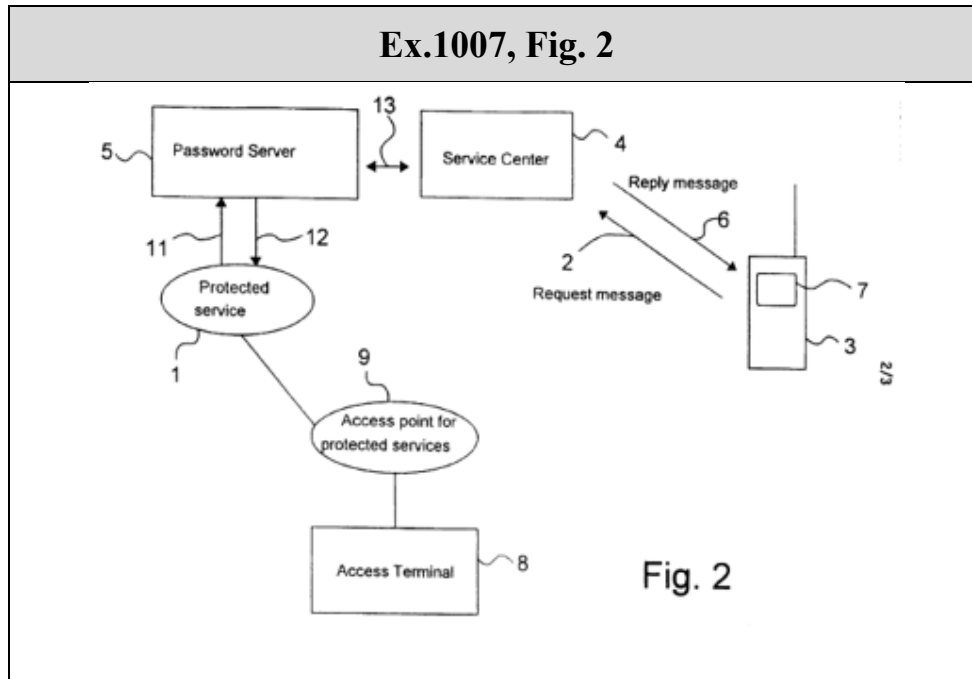


57. I understand that in response, the system “requests authentication via an authentication challenge network 28 by sending a challenge code...to the user’s personal unit 20.” *Id.*, 10:23-27. The user is then prompted “to input, for example, a security code, such as a PIN,” and, once entered, “the personal unit 20 calculates

and sends a response code...to the display.” *Id.*, 10:29-33. I understand *Jonsson*’s algorithm “calculates a response code based on the received challenge code, the user input (e.g., PIN), and optionally the secret key.” *Id.*, 8:12-14, 7:5-10, 9:23-25. The user “manually inputs the displayed response code to the terminal 22,” where it is transmitted via the service access network 24 to the service node 26, and authentication center 30 “compar[es]...the received response code to the expected response code.” *Id.*, 11:4-20.

### **3. Sormunen (Ex.1007)**

56. A POSITA would understand *Sormunen* discloses authenticating a user to access network resources based on a dynamic password submitted via an access terminal. Ex.1007, 7:9-18. To increase security, I understand *Sormunen* discloses a method of obtaining the dynamic password that includes a three-step and three-device architecture: (1) sending a “password request” from the user via a mobile station (first device) to a password server (second device), (2) transmitting the password to the mobile phone over a mobile communication network, and (3) submitting the password to the password server via an access terminal (third device) for authentication. *Id.*, 5:33-7:18, Fig. 2.



57. It is my opinion that having a “request [] transmitted by the user through the personal communication device,” which claim 7 recites, is nothing new (as *Sormunen* demonstrates).

#### **4. Kaufman (Ex.1008)**

58. A POSITA would understand *Kaufman* discloses “a workstation [that] exchanges data with an authentication server to obtain access to a desired computing system.” Ex.1008, 6:50-52. In *Kaufman*, “the user initiates communications with the authentication server by entering his ‘password’ into the workstation” and “enters a token provided by the passive token generator.” *Id.*, 6:66-7:2. The workstation then “calculates a ‘transmission code’ by applying a

first, cryptographically secure hashing algorithm to the password and the token, so that this information can be securely sent to the server.” *Id.*, 7:2-5.

59. As disclosed in *Kaufman*, the “hashing algorithms,” shown in the portion of *Kaufman* I have reproduced below, are used to describe “a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data.” *Id.*, 9:43-47.

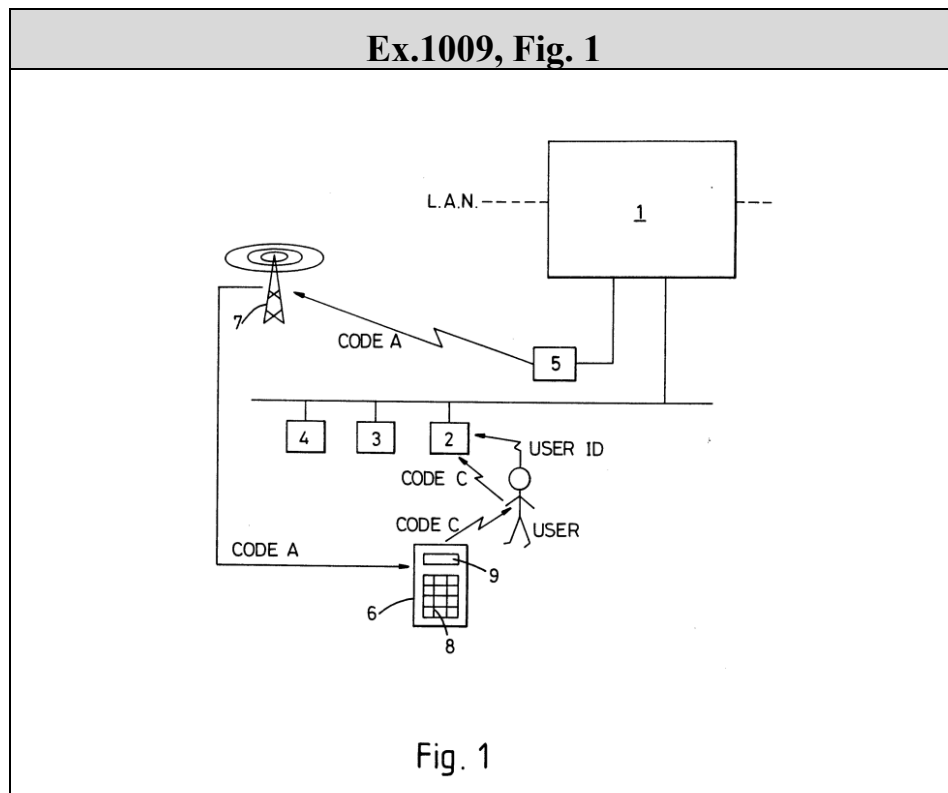
| Ex.1008, 9:65-10:5 – Hashing Algorithms Disclosed in <i>Kaufman</i> |                              |
|---------------------------------------------------------------------|------------------------------|
| [1.0]                                                               | hash(token   hash(password))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

60. As I explain in detail below, in my opinion *Kaufman* teaches the “concatenating” requirements of claim 2.

## 5. Kew (Ex.1009)

61. A POSITA would understand *Kew* discloses “a method of preventing unauthorized access to a host computer system (1) by a user at a remote terminal (2) ...using paging system technology.” Ex.1009, Abstract, Fig.1; *see id.*, 7:34-9:11, Fig. 2. I note that, as shown below in *Kew*’s Figure 1, a user enters an identification code (e.g., a name or PIN) into a terminal (e.g., elements 2, 3, 4 in Figure 1) to gain access to a host computer system 1. Ex.1009, 7:34-8:2. A

security server 5 that “includes a database of all authori[z]ed users and their authori[z]ed receiver units 6,...generates a random code (Code A).” *Id.*, 8:2-6. I understand security server 5 then (1) uses the random code and the identification code to produce a new transformed Code B, and (2) “transmits the random code to a paging system 7 along with an identifier or identifying tag which can be recognized by the receiver unit 6.” *Id.*, 8:5-23. Once receiver unit 6 receives random Code A, it “uses the received random number and the identity code stored in its own EPROM to produce a transformed code (Code C) via [the receiver unit’s] own characteristic algorithm,” which is the same as the one used by security server 5 to produce transformed code (Code B). *Id.*, 8:33-36, Fig. 2.



62. “This transformed Code C is then displayed to the user...for a predetermined length of time.” *Id.*, 8:33-9:3. The user inputs transformed Code C into receiver unit 6 and “security server 5 compares the input Code C with the transformed code, Code B, it produced by encryption of the random code, Code A.” *Id.*, 9:5-11. I understand that if Code C matches Code B, the user is granted access. *Id.*, 9:9-11.

63. These brief background summaries are provided as general overviews. I provide detailed opinions below concerning how combinations of these references render obvious claims 2 and 7. Let me now turn to a discussion of those specific opinions.

**VII. MY OPINIONS AS TO *VENEKLASE*, *JONSSON*, AND *SORMUNEN* AND THE OBVIOUSNESS OF CLAIM 7**

64. Claim 7 depends from claim 6, which depends from claim 5.<sup>2</sup> In my opinion, *Veneklase*, in view of *Jonsson* and *Sormunen*, renders the limitations of

---

<sup>2</sup> In discussing claim 7, I will first consider independent claim 5 of the '658 Patent since those limitations form a part of claim 5 by virtue of the claim dependencies. In my opinion, claim 5 does not explicitly require that a user request the token via a personal communication device, which is a limitation added by challenged claim 7. I understand that claim 1 is a method claim with similar limitations to claim 5

claims 5 and 6 obvious, as I discuss below. Claim 7 adds that the “request is transmitted by the user through the personal communication device,” which is abundantly obvious.

**A. Claim 5**

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

65. I have been informed that claim preambles are generally not limiting. In any case, to the extent it is limiting, I believe *Veneklase* discloses the preamble. *Veneklase* discloses “[s]everal embodiments of computer security systems [that] are adapted to grant an authorized individual access to a secured domain, such as a computer or data stream.” Ex.1005, Abstract, Fig. 6.

66. It is therefore my opinion that *Veneklase* discloses “a user authentication system.”

---

and, like claim 7, requires that the system receive a token request from a user via a cell phone network.

**Ex.1005, Fig. 6 (annotated)**

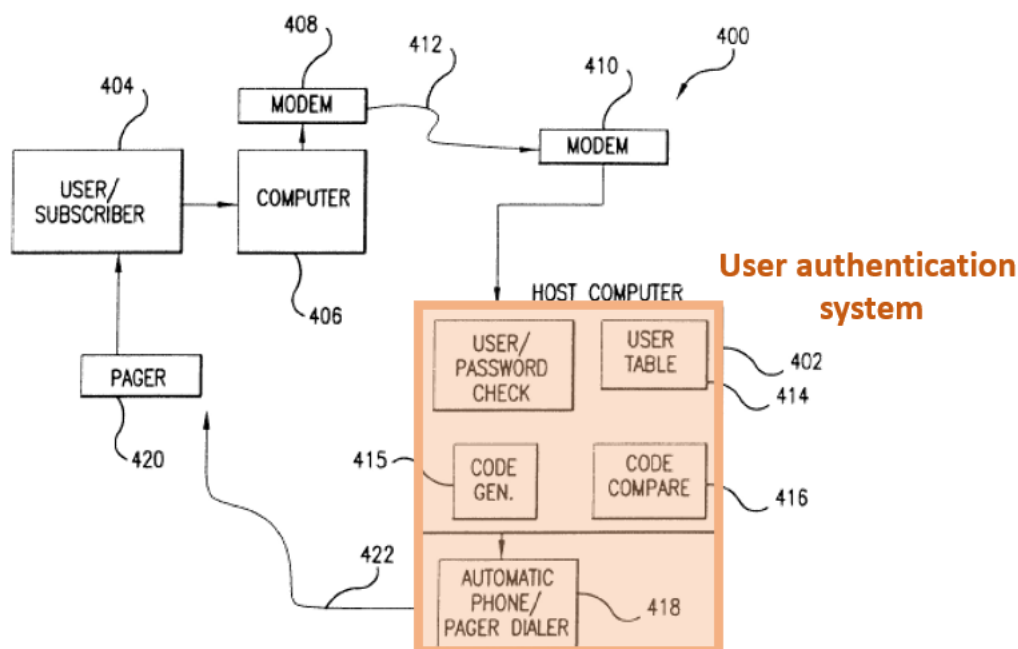


**FIG.6**

**2. Claim 5[a]— “a computer processor;”**

67. *Veneklas* teaches this limitation. *Veneklas* discloses that its authentication system operates in host computer 402. Ex.1005, 7:29-8:27, Fig. 6. *Veneklas* further discloses that computer 80, which corresponds to computer 402, can “comprise a microprocessor and/or similar type of computer which operates under stored program control.” *Id.* 5:55-6:4, 7:34-39, Fig. 1.

Ex.1005, Fig. 6 (annotated)

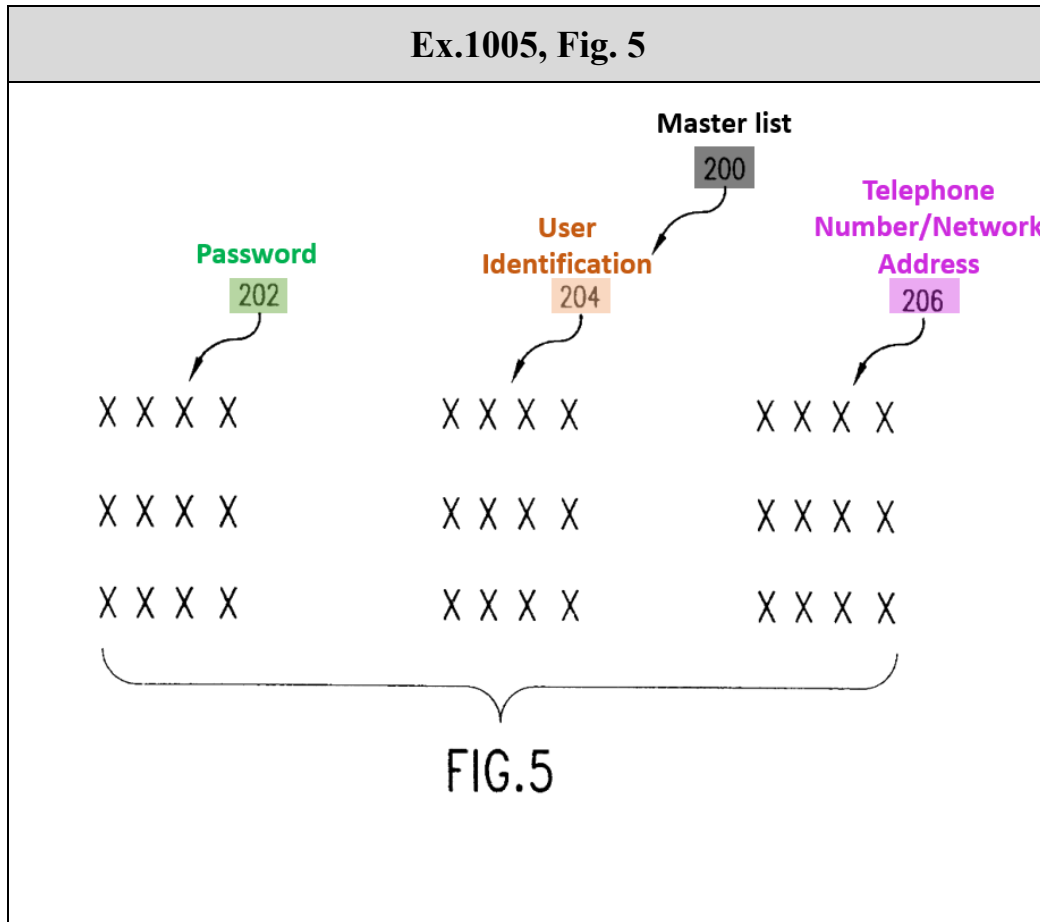
FIG. 6

69. In my opinion, *Veneklase* therefore discloses “a computer processor.”

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

70. I believe *Veneklase* teaches or renders obvious this limitation.

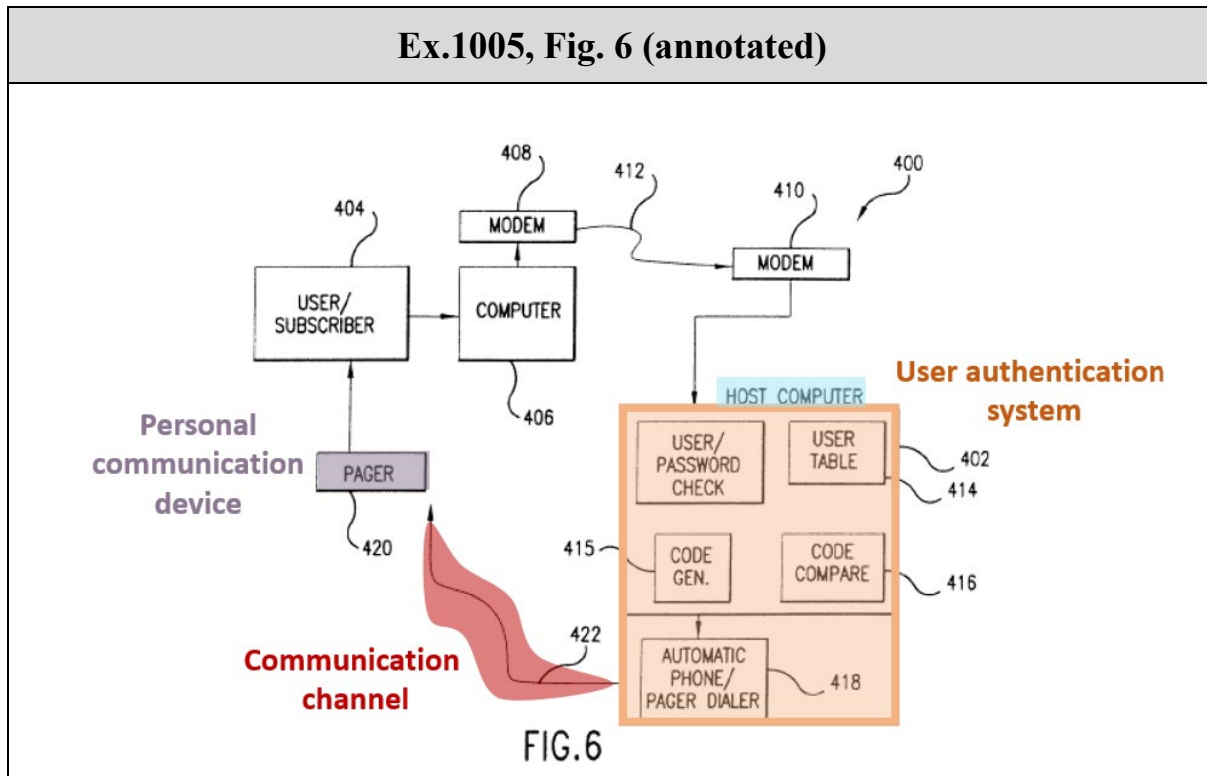
*Veneklase* discloses that “host computer 402 checks the received identification code and cross references the received password code against a pager phone number list resident within the user table 414 which is stored within computer 402.” Ex.1005, 8:1-5, Fig.6. As shown in an annotated version of Figure 5 below, “each authorized password 202, contained in this master password list 200, has a unique first entry 204 associated with it and which **identifies the name of the authorized user who has been assigned that corresponding password and at least one telephone number 206 and/or network address associated with the identified user.**” *Id.* 6:15-26.



71. A POSITA would understand that *Veneklase*'s association of a telephone number with user identification 204 and a personal communication device (e.g., a pager) is just like what the '658 Patent discloses. *Compare* Ex.1005, 8:1-5, with Ex.1001, 2:17-18 ("The method includes associating a user ID with a phone number of a personal communication device."). Upon determining that the received user identification 204 is matched with a telephone number, *Veneklase*'s "automatic dialer 418 telephones the conventional and commercially available pager 420 by means of **conventional and commercially available communication channel 422 (e.g. voice line).**" Ex.1005, 8:5-14.

Amazon.com – Ex.1002

72. I understand that *Veneklase*'s disclosed personal communication device (e.g., pager 420) is configured to communicate with the user authentication system (e.g., host computer 402) over a cell phone network (e.g., communication channel 422). For example, I note in Figure 6 that communication channel 422 allows the personal communication device (e.g., pager 420) to communicate with the user authentication system (e.g., host computer 402) using the automatic phone/pager dialer 418. See Ex.1005, Fig. 6.



73. *Veneklase* explains that the communication channel over which the random code is sent could be a “**communications channel 84 [that] comprises a pager or cellular phone.**” *Id.*, 8:55-58. A POSITA would have understood that

the “conventional and commercially available communication channel 422” described in *Veneklase* discloses the claimed “cell phone network,” which is consistent with the ’658 Patent’s repeated statements that such a cell phone network can communicate with cell phones and/or pagers. *See, e.g.*, Ex.1001, 5:32-40 (“The communication module 118 forwards tokens 156 to a text-messaging service provider 104, which may be a pager or mobile phone service provider.”), Abstract, 1:10-11, 2:6-8, 2:28-31, 3:1-3, 4:13-17, 9:45-54.

74. Furthermore, *Veneklase* discloses that the communication channel over which the random code is sent could be a pager or a cell phone, stating that “the predetermined period of time would be shorter when **communications channel 84 comprises a pager or cellular phone**, since the owner has immediate access to the code upon transmission.” Ex.1005, 8:55-58. Thus, a POSITA would have understood that communication channel 422 meets the requirements of a cell phone network as claimed in the ’658 Patent, e.g., a mobile device or pager service provider communication network.

75. To the extent it is argued that *Veneklase* does not disclose a cell phone network, a POSITA would have found it obvious to implement the authentication system of *Veneklase* using a cell phone network. *Veneklase* explicitly contemplates using cellular phones instead of pagers. Ex.1005, 8:55-58. *Veneklase* further explains that utilizing “communications channel 84” to

communicate with a cellular phone could reduce the predetermined period before which a password would expire because the use of a cellular phone would allow the user to “ha[ve] immediate access to the code upon transmission.” *Id.* A POSITA would have recognized that this would increase security (e.g., by reducing times during which a password could be stolen and used) and user convenience (e.g., by displaying passwords instantaneously on cellular phones already carried by the user and, have a wide range of functionality and provide often larger, easier to view screens as compared to pager devices in the relevant time period). In addition, it would have been obvious to use a cell phone network to send *Veneklase*’s random code because doing so would be a simple substitution of one known element (e.g., pager network) for another (e.g., cell phone network) and would have made the system available to more users having different types of devices and in more locations, which is one of *Veneklase*’s objectives. Ex.1005, 1:15-49. A POSITA would have had a reasonable expectation of success in modifying *Veneklase*’s authentication system to use a cellular network instead of a pager network because these networks operate similarly, often using the same protocols, such that the modification would have merely involved swapping out devices and making rudimentary software configuration changes.

76. In my opinion, *Veneklase* therefore teaches *a user database configured to associate a user with a personal communication device possessed by*

*the user* (e.g., user table 414 that associates the name of the authorized user with at least one telephone number), *said personal communication device* (e.g., pager 420 and/or the cellular phones of *Veneklase*) *configured to communicate over a cell phone network* (e.g., communication channel 422) *with the user authentication system* (e.g., host computer 402).<sup>3</sup>

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

77. In my opinion, *Veneklase* in combination with *Jonsson* renders this limitation obvious. *Veneklase* discloses “the steps of assigning a password to the user; receiving the password by use of a first communications channel; generating a code in response to the received password; transmitting the code by use of a second communications channel to the user; transmitting the code to the computer; and allowing access to the computer only after the code is transmitted to the computer.” Ex.1005, 4:8-15.

78. A POSITA would have understood that *Veneklase* discloses a “user/password check” module (i.e., a control module) located on the host

---

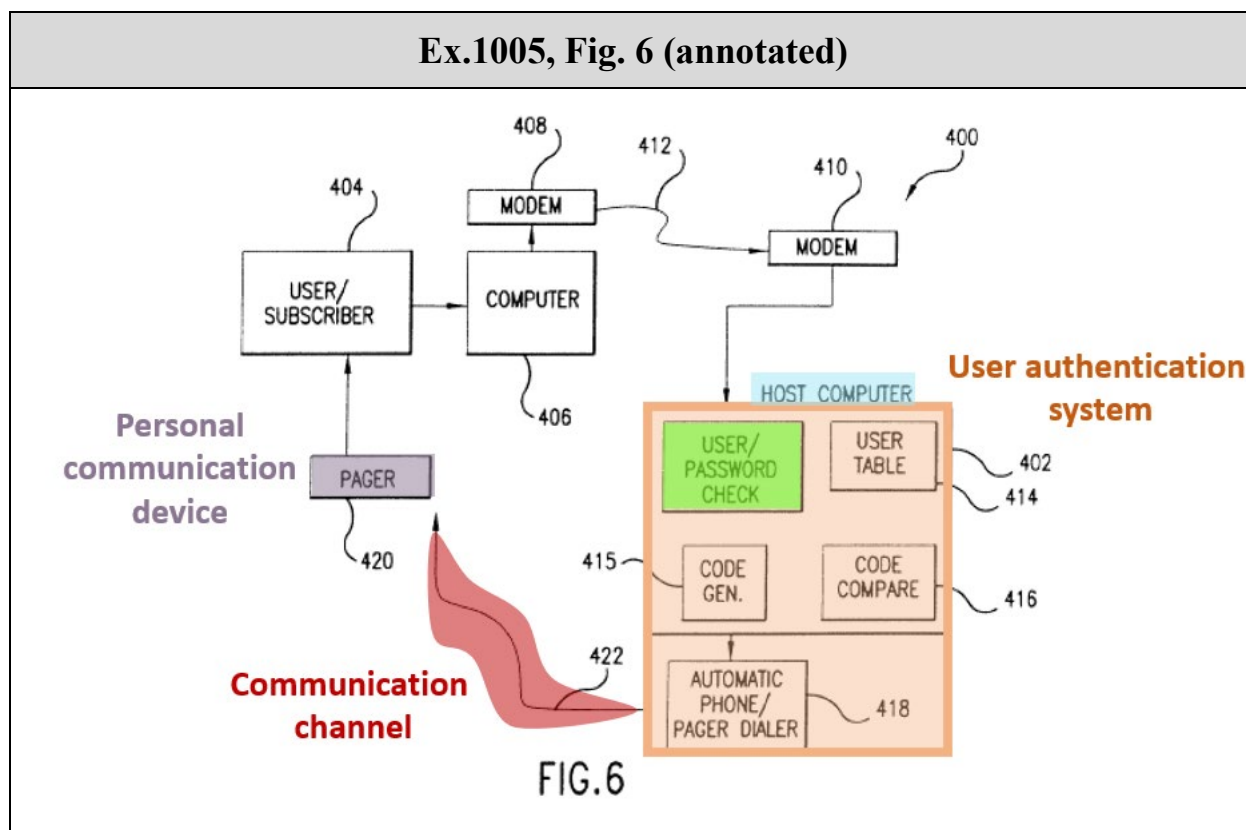
<sup>3</sup> In this Declaration I have italicized claim language throughout my discussion.

computer system 402 (i.e., the computer processor). *See* Ex.1005, 7:55-8:5, Fig. 6; *see also id.*, 6:10-14.<sup>4</sup>

---

<sup>4</sup> I understand that the Unified IPR identified a means-plus-function structure for “control module.” Ex.1012, 12-13. For purposes of this proceeding only, I have identified that same corresponding structure. Ex.1001, 2:32-48, 8:2-8, 8:53-9:44, Figs. 1, 4, 5. As I explain in this section, that corresponding structure is present in the cited combination for the functional aspects, and the cited combination also includes “software executed on a ‘server’ that: (1) associates user ID with passcode and phone number of user’s personal communication device, (2) generates a new password, and (3) sets or rests the password associated with the user ID.”

Ex.1005, Fig. 6 (annotated)



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

80. While *Veneklase* teaches an authentication system in which the user inputs both a token that is not known to the user beforehand (e.g., random code) and a passcode that is known to the user (e.g., received password), I do not believe it explicitly discloses creating a new password based on those two items.

However, it would have been obvious for a POSITA to combine those two steps and create a new password based on both items.

81. For instance, I note that *Jonsson* discloses a system that includes a service node that “generates a challenge code and requests that the challenge code be sent to the personal unit 20 via an authentication challenge network 28.”

Ex.1006, 4:24-5:6, 9:9-25. A POSITA would have understood the challenge code is a *token* because it is not previously known to the user before it is generated and sent to the user. Additionally, *Jonsson* discloses the use of a “user input such as a personal identification number (PIN),” which is already known to the user. *See* Ex.1006, 3:3-10, 3:14-18, 7:32-8:11. Indeed, *Jonsson* discloses that the challenge code is “unique for each transaction” and “the PIN or other user input may be changed from time to time.” Ex.1006, 3:14-18, 7:32-8:11 (“the user input, such as a PIN, can be updated at the user’s discretion or on a regular basis”).

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

that “[t]his provides a triple check on the identity of the user, requiring information from three separate sources (user: PIN, service node or authentication center: challenge code, and provider of the personal unit: secret key), thereby increasing the relative security of the transaction against fraud or other unauthorized use.” *Id.*, 7:18-23.

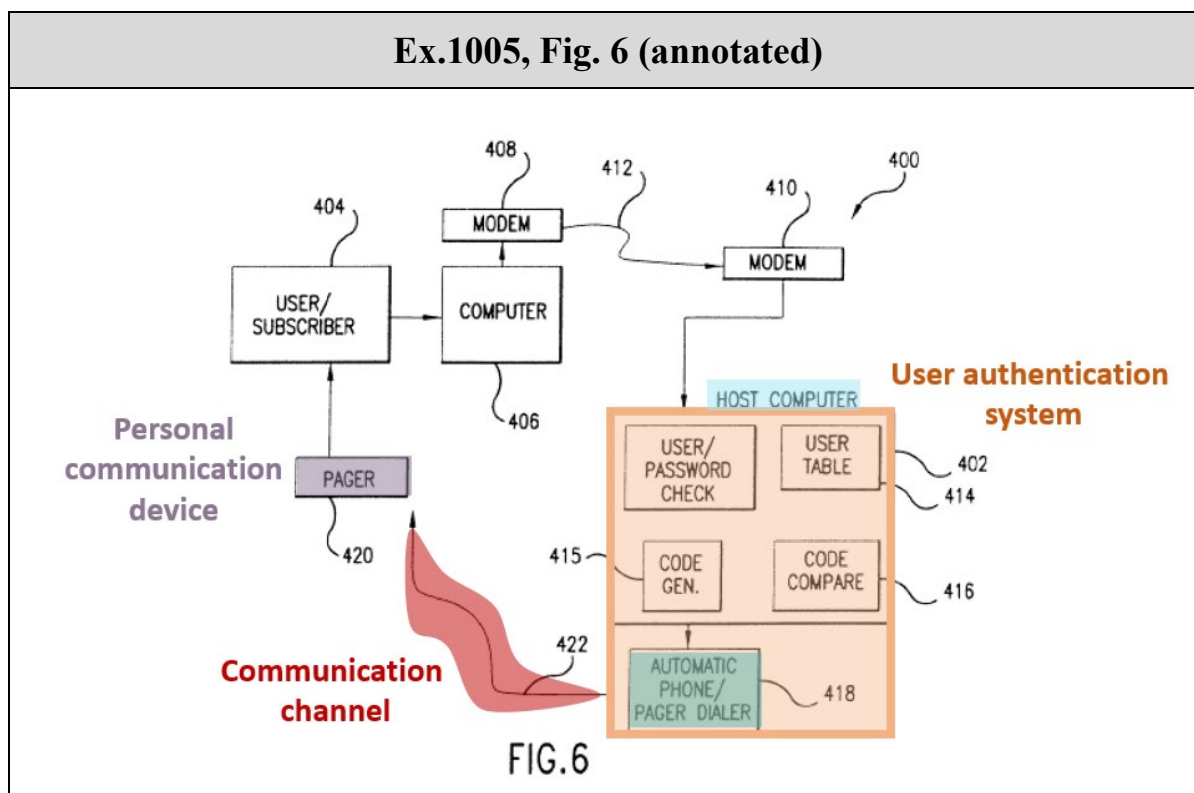
83. Additionally, *Jonsson* discloses that “[t]he response code is compared to an **expected response code [i.e., a created new password]**, which, in **exemplary embodiments, may be pre-stored [i.e., set as the new password]** or generated using the same algorithm and variables.” *Id.*, 10:2-5. *Jonsson* explains that “[t]he response code is to be **unique to each transaction**,” and a POSITA would have understood that this pre-stored expected response code is a new password associated with the user. *Id.*, 7:34-35. This understanding is also consistent with the prosecution history for the ’658 Patent. *See* Ex.1004, 195-96 (applicant traversing prior art for not having a response code that is unique to each transaction).

84. In my opinion, in *combination*, the authentication system in *Veneklas* would incorporate *Jonsson*’s teachings to use an algorithm to create a new password (e.g., response code) based on a known passcode (e.g., *Veneklas*’s received password/*Jonsson*’s PIN) and an unknown token (e.g., *Veneklas*’s random code/*Jonsson*’s challenge code).

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

85. In my opinion, *Veneklase* teaches or renders obvious this limitation.

As I explained above in Section VII.A.3, which I incorporate here, *Veneklase*’s communication channel 422 discloses or renders obvious the claimed cell phone network. *Veneklase*’s discloses that “host computer 402 checks the received identification code and cross references the received password code against a pager phone number list resident within the user table 414 which is stored within computer 402.” Ex.1005, 8:1-5. I understand that after *Veneklase*’s system correlates an identification code with a user’s phone number, a random number code is generated and passed “to the commercially available and conventional automatic dialer 418,” which “telephones the conventional and commercially available pager 420 by means of conventional and commercially available communication channel 422 (e.g., voice line) and transmits the code to the user’s pager.” Ex.1005, 7:52-8:17, Fig. 6.



86. A POSITA would have recognized that *Veneklas*’s automatic phone/pager discloses the claimed communication module, and that the claimed cell phone network can support both pagers and cellular phones. *See, e.g.*, Ex.1001, 10:31-34 (“the communication module 118 is a phone dialer 622”), 5:32-40, Abstract, 1:10-11, 2:6-8, 2:28-31, 3:1-3, 4:13-17, 9:45-54.<sup>5</sup>

<sup>5</sup> I understand the Unified IPR identified a means-plus-function structure for “communication module.” Ex.1012, 13. For purposes of this proceeding only, I identify the same corresponding structure. Ex.1001, 2:39-42, 5:66-6:1, 6:18-20, 10:14-41, Fig. 1. As I explain herein, that corresponding structure is present in the

87. In my opinion, *Veneklase* therefore teaches *a communication module* (e.g., automatic phone/pager dialer 418) *configured to transmit the token to the personal communication device through the cell phone network* (e.g., transmit the random code through communication channel 422).

**6. Claim 5[e]— “an authentication module configured to receive the password from the user through a secure computer network, said secure computer network being different from the cell phone network,”**

88. In my opinion, *Veneklase*, alone or in combination with *Jonsson*, teaches or renders obvious this limitation. *Veneklase* discloses *an authentication module* (e.g., code compare module 416) *configured to receive the password from the user through a secure computer network* (e.g., by receiving the random code via a typical communication channel 412). Specifically, *Veneklase* discloses that “user 404 now enters the code he or she has received from the pager 420 . . . and **sends this password or pseudo-random code back to computer 402 where it is compared within the software subroutine module denoted as ‘code compare’ 416.**” Ex.1005, 8:18-27, 3:50-4:3. *Veneklase* further discloses that its system will

---

cited combination for the functional aspects, and the cited combination also includes a “(1) a mobile device with messaging capabilities, (2) a phone dialer, or (3) a connection card connected to a messaging service provider.”

“allow that individual access to the computer system only if that individual generates and communicates the code to the code generation means.” *Id.*, 4:1-3.

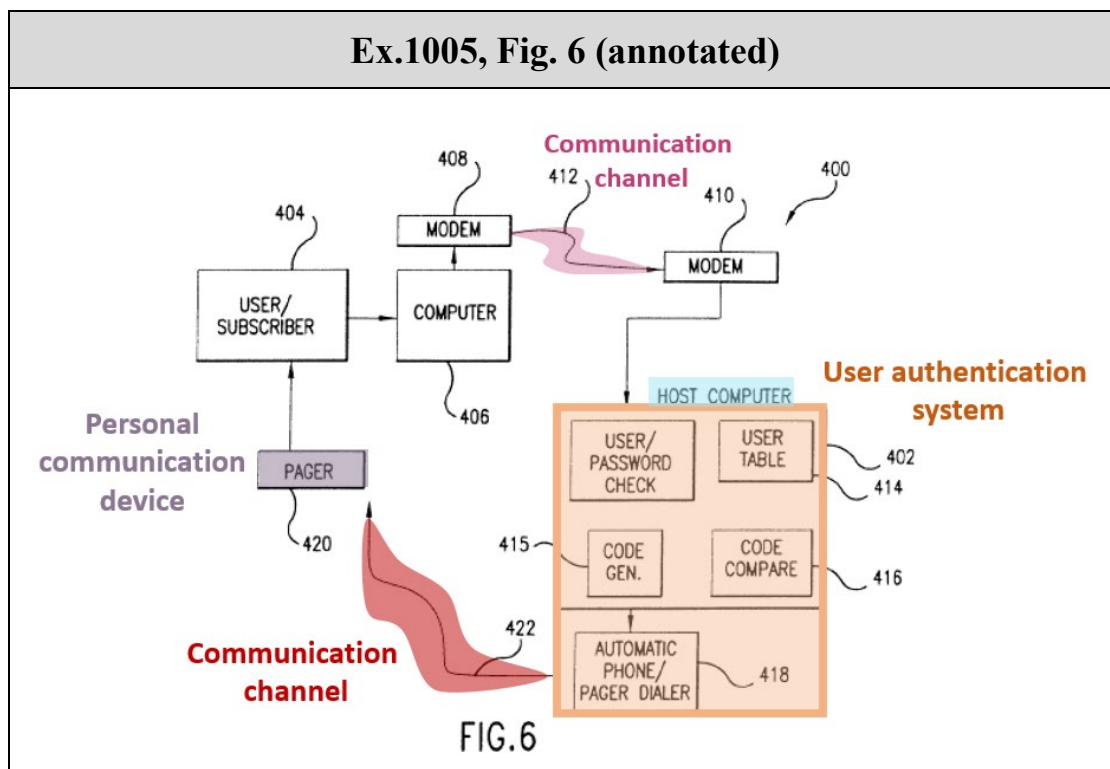
89. In combination with *Jonsson*, a POSITA would have understood that the new password (*i.e.*, response code) being sent back to computer 402 and compared against the expected response code is the one created by the algorithm based on both the known passcode (*i.e.*, *Veneklase*’s received password/*Jonsson*’s PIN) and the randomly generated token (*i.e.*, *Veneklase*’s random code/*Jonsson*’s challenge code).<sup>6</sup>

90. I understand that *Veneklase* also discloses *said secure computer network* (e.g., typical communication channel 412) *being different from the cell phone network* (e.g., a channel different from communication channel 422).

---

<sup>6</sup> I understand the Unified IPR identified a means-plus-function structure for “authentication module.” Ex.1012, 13-14. For purposes of this proceeding only, I have identified the same corresponding structure. Ex.1001, 3:4-25, 5:3-10. Fig. 1. As I explain herein, that corresponding structure is present in the cited combination for the functional aspects, and the cited combination also includes “software executed on a ‘server’ that: (1) receives a submitted password in response to a request for authentication and (2) grants access to the user if the submitted password matches the valid password.”

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



91. In my opinion, a POSITA would have understood that this communication network is *a secure computer network* because the authentication procedures employed in *Veneklase* make the host computer system more secure. *See, e.g., id.*, 9:3-14 (describing host computer as “the secure domain”). I note that this is similar to what the ’658 Patent describes, which is “for a secure system, such as a computer system.” *See* Ex.1001, 1:63-65, 2:49-3:3, 4:9-26, 10:30-41 (“In this case, the communication module 118 is a phone dialer 622, the personal communication device 106 is a pager 624, and the text messaging Service provider is a paging Service 626. In order to transmit a token 156, the phone dialer 622 places a phone call 623 to the phone number of the user’s pager 624.”).

92. In my opinion, *Veneklase*, either alone or in combination with *Jonsson*, teaches *an authentication module* (e.g., code compare module 416) *configured to receive the password from the user through a secure computer network* (e.g., by receiving the password via a typical communication channel 412), *said secure computer network being different from the cell phone network* (e.g., a distinct communication channel different from communication channel 422).

7. **Claim 5[f]— “wherein the user has an account on the secure computer network, wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account, such that said account is not accessible through any password via a secure computer network.”**

93. In my opinion, *Veneklase*, in combination with *Jonsson*, renders obvious this limitation.

94. ***Activates Access – Unified IPR Board’s Construction.*** I understand that the Board in the Unified IPR rejected Petitioner’s arguments and stated that “Claim 5 ... does not require that the account be activated in response to creation of the password.” Ex.1013 (Unified Institution Decision), Paper 9 at 24. I understand that this construction for claim 5 was different than that identified by the district court, due in large part to the district court relying on disclaimers made by the Patent Owner during the Unified IPR. But this makes no difference to my opinions as the references I rely on here teach the claim under either the Board’s construction (discussed in the next sentences) or the district court’s construction (discussed below). *Veneklase* discloses *wherein the authentication module* (e.g., code compare module 416) *activates access to the account in response to the password* (e.g., allows access if the random codes match). Specifically, *Veneklase* discloses that the user 404 “sends this password or pseudo-random code back to computer 402 where it is **compared within the software subroutine module**

denoted as ‘code compare’ 416 in Figure 6” and, “[i]f the comparison yields a match, the user 404 is allowed access to computer 402 and/or to a portion of computer 402.” Ex.1005, 8:18-27, 6:45-7:10.

95. *Activates Access – District Court’s Construction.* As I mentioned above, I understand that Judge Payne during the district court case construed this phrase to mean “activates access to the account in response to the creation of the password.” Ex.1011, 16. In my opinion, *Veneklase* in view of *Jonsson* still renders this limitation obvious. As I noted above, *Jonsson* discloses creating “an expected response code [*i.e.*, a created new password], which, in exemplary embodiments, may be pre-stored [*i.e.*, set as the new password] or generated using the same algorithm and variables.” Ex.1005, 10:2-5. *Jonsson* explains that “[t]he response code is to be **unique to each transaction**,” and a POSITA would have understood that this pre-stored expected response code in the combined *Veneklase-Jonsson* system is a *new password* associated with the user. *Id.*, 7:34-35. A POSITA would have recognized that it would have been obvious to activate access to the account in response to *Jonsson*’s generation and storage of the expected response code so as to enable a user to immediately access their account after they were verified as the sole requester of that response code. At a minimum, this would have been obvious to try for the simple reason that it was one of a finite number of options, *i.e.*, whether to immediately activate an account in response to

the expected response code or wait a period of time before activating the account. Such a finite number of available options would have lent themselves to be attempted by a POSITA, and success would have been reasonably expected as activating the account at different points in time was well within the skill of a POSITA through routine software updates and/or optimizations.

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

97. *Veneklase* also further discloses that its system *deactivates the account within a predetermined amount of time after activating the account* (e.g., denies entry if the random code is not received in the predetermined time window), *such that said account is not accessible through any password via the secure computer network* (e.g., not accessible without the random code). I understand that *Veneklase* “includes a timer or ‘timing means’ 40” that can “operate and/or execute

within and/or upon computer 80,” such as a watchdog timer. Ex.1005, 8:28-39.

The “timing means 40 records the time at which the first and second passwords are received by analyzing means 12” and “then compares the times to determine whether the second password [sent to the cellular phone] was received **within a predetermined period** or predetermined ‘window’ of time after the first password [*i.e.*, the expected response code] was received,” which corresponds to the time at which it was created and activated the account. *Id.*, 8:40-49. “If the second password [sent to the cellular phone] was not received within the predetermined period of time, analyzing means 12 denies entry to the secured domain (e.g., computer 80).” *Id.*, 9:3-6. A POSITA would have understood that this denial of entry to the secured domain (*i.e.*, deactivating of the account) occurs regardless of whether the user might know or guess the correct password (since the reference teaches that once the predetermined period of time expires, entry is denied and there are no caveats to that denial of entry), and thus **said account is not accessible through any password via the secure computer network.**

98. In combination with *Jonsson*, I believe a POSITA would have understood that the new password (e.g., response code) being sent back to computer 402 and compared against the expected response code is the one created by the algorithm based on both the known passcode (e.g., PIN) and the randomly generated token (*e.g.*, challenge code). I observe that the predetermined period

would thus be the time allowed after generation of the expected response code and/or of the new password by the personal communication device (which a POSITA would have understood occurs at or around the same time) for the user to enter and send the new password to computer 402. *Id.*

99. I note that *Veneklase* discloses the claimed deactivating limitation because the teaching is nearly identical to how this limitation is described in the '658 Patent. *See* Ex.1001, Fig. 5, 9:61-64. Indeed, the '658 Patent discloses in Figure 5 that the “user can access secure system by logging in using token” in step 516, but if the “token expires” in step 518, it “deactivate[s] user account in user database.” Ex.1001, Fig. 5, 9:61-64 (“At a step 518, if the token has an expiry time, the token 156 expires. At a step 520, upon expiration of the token 156, the control module 402 deactivates the user account in the user database 114.”).

100. In my opinion, *Veneklase*, in combination with *Jonsson*, therefore teaches *wherein the user has an account on the secure computer network* (e.g., the user’s password associated with an account is found on the master password list), wherein the authentication module (e.g., code compare module 416) *activates access to the account in response to the password* (e.g., allows access to and/or activates the account itself, if the response codes match) *and deactivates the account within a predetermined amount of time after activating the account* (e.g., denies entry if not received in the predetermined time window), *such that said*

*account is not accessible through any password via the secure computer network*  
(e.g., not accessible even with the right password).

**B. A POSITA Would Have Been Motivated to Combine *Veneklase* and *Jonsson***

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

102. *Veneklase* and *Jonsson* are analogous art and in the same field of endeavor as the '658 Patent because all three relate to authentication systems with personal communication devices. I note that a POSITA would have appreciated that all references are within the same field of endeavor and address similar problems as in each other and the '658 Patent. *See* Ex.1001, 1:7-11 (discussing systems for "authentication of users of secure systems and...system[s] through which user tokens required for user authentication are supplied through personal communication devices"). *Veneklase* discloses "computer security systems...which are adapted to grant an authorized individual access to a secured domain" by use of a pager. Ex.1005, Abstract. Like *Veneklase*, *Jonsson* discloses "[a]uthorization for a user to use a service is provided by a modified pager."

Ex.1006, Abstract. All references are also reasonably pertinent to the same problem, e.g., improving security.

103. I further note that both references are particularly pertinent to another aspect of the '658 Patent's teachings of authenticating user access "using a device that many users already carry," e.g., "a mobile phone or a pager." Ex.1001, 1:56-59. *Veneklas* discloses the same solution of using a mobile device for authentication. Ex.1005, 8:5-15. *Jonsson* likewise avoids the shortcomings of prior art systems "requir[ing] specially equipped, and often dedicated, terminals, which raises the cost and reduces the availability of the associated electronic service." Ex.1006, 2:8-14.

104. A POSITA would have been motivated to combine *Veneklas* and *Jonsson* because having only one password transmitted via computer system is more efficient, secure, and convenient. *Veneklas* teaches a system in which a user inputs a password known beforehand; receives a randomly generated, previously unknown code; and then inputs that for authentication purposes. *See, e.g.,* Ex.1005, 7:52-8:27. *Jonsson* discloses a similar authentication system that involves the user inputting a known PIN. *See, e.g.,* Ex.1006, 10:22-31. *Jonsson* discloses an algorithm that "calculates a response code based on the received challenge code, [and] the user input (e.g., PIN)." *Id.*, 8:12-14. *Veneklas*'s system allows for authentication through user input of a known and unknown code at

separate times through the secure computer network in a two-step process, and in my opinion, a POSITA would have been motivated to look to *Jonsson* in seeking to further simplify *Veneklase*'s authentication scheme and also save time for users, which could have provided the added benefit of reducing what needs to be entered through the secure computer network to a single step (*i.e.*, single entry of the generated response code).

105. A POSITA would have been motivated to combine *Veneklase* and *Jonsson* because implementing the algorithm of *Jonsson*'s system in *Veneklase*'s authentication system provides an additional layer of security. For example, a POSITA would have understood that implementing *Jonsson*'s algorithm system would provide the added security benefit of preventing unauthorized personnel from being able to access the system by engaging in SIM swapping. Ex.1006, 2:30-3:18. SIM swapping was a well-known method in the relevant time period that was used by hackers in which they contacted a user's service provider and activated a new SIM card on a different device in order to receive the user's authentication token. A hacker's attempt to do so would not work in the combined system, as they would need access to the device containing the algorithm. *Id.*

106. In my opinion, *Veneklase* explicitly provides a teaching, suggestion, and motivation for combining it with an authentication system that uses an algorithm, such as that taught in *Jonsson*, because it explicitly discloses

embodiments in which data streams are encoded and decoded using algorithms for additional security. *See* Ex.1005, 9:26-10:11. Thus, a POSITA would have been motivated to use an algorithm for creating a new password based on the known password and the previously unknown randomly generated code, as described in *Jonsson*, for additional security.

107. While *Veneklase* mentions certain weaknesses of encryption algorithms in the background section, I note that this is in the context of “modifying and/or changing the transmitted data in a certain manner, and/or requiring the transmission and receipt of modified data before access is granted.” Ex.1005, 2:37-56. These drawbacks would not apply in the context of the algorithm for creating a new password disclosed in *Jonsson* because it would not “provide[] all of the transmitted data, in some form.” *Id.*; Ex.1006, 10:22-27. In other words, the drawbacks noted in *Veneklase* are directed to encrypting all of the data as compared to using encryption to create a new password to access the data. Additionally, the combination would still utilize all of the protections provided for in *Veneklase*, so it is my opinion that additional security would then have been provided (not less). *Id.*

108. *Jonsson* clearly discloses that “[t]he specific algorithm used in a given embodiment is not germane to the present invention,” and “[a]lgorithms of this type are known in the art or readily derived therefrom” (Ex.1006, 7:10-14), so I do

not believe a POSITA would have been concerned about the cost or complexity of such algorithms.

109. A POSITA would have been motivated to combine *Veneklase* and *Jonsson* because the combination merely uses a known technique to improve similar devices in the same way. For example, I believe a POSITA would have been motivated to utilize the algorithm of *Jonsson* in the system of *Veneklase* because it would have been used in the same way, *i.e.*, to provide another layer of security. Ex.1006, 7:5-17. *Veneklase* discloses the use of known passwords and previously unknown randomly generated codes, so it would have been obvious for a POSITA to combine the two inputs.

110. In my opinion, a POSITA would have had a reasonable expectation of success modifying *Veneklase*'s authentication system, which requires the use of both a known password and a previously unknown randomly generated code, to create a new password based on those two values, as taught by *Jonsson*, because doing so would have merely made two steps into one without requiring any additional hardware (or alternatively *Jonsson*'s PIN and generated response code could also have been easily incorporated into *Veneklase*'s system). Therefore, a POSITA would have been motivated to combine, and would have had a reasonable expectation of success in combining, *Veneklase*'s teachings, including a control module executed on the computer processor configured to create a token and a

passcode, wherein the token is not known to the user and wherein the passcode is known to the user, with *Jonsson*'s teaching related to creating and setting a new password based at least upon the token and setting that new password to be the new password.

**C. Claim 6**

111. Claim 6 depends from claim 5, which I believe is obvious in view of *Veneklase* and *Jonsson* as I discussed above in Sections VII.A-B and will avoid repeating here for the sake of brevity. Claim 6 adds: “*wherein the communication module is further configured to receive a request from the user for the token, and wherein the control module is further configured to create the new password in response to the request.*”

112. In my opinion, *Veneklase* in combination with *Jonsson* renders this limitation obvious. *Veneklase* discloses a user/password check module (*i.e.*, a control module), and a POSITA would have understood that the user's submission of the password through the first communications channel is a request from the user for the token (e.g., generating a code in response to the received password). Ex.1005, 7:55-8:5, Fig. 6, 4:7-12. While *Veneklase* does not expressly disclose that the control module is configured to create a new password in response to the user's request, it would have been obvious to a POSITA to modify this module to perform that function.

113. I observe that a POSITA would look to a reference such as *Jonsson*, which discloses a similar authentication system that is *further configured to receive a request from the user for the token (i.e., the service node receives the user's request and then generates a token or challenge code in the node or an authentication center) and wherein the control module is further configured to create the new password in response to the request (i.e., the expected response code used for the comparison)*. Ex.1006, 9:2-7, 10:2-5. Specifically, *Jonsson* discloses that the user requests “access through terminal 22 by transmitting the request over a service access network 24 to a service node 26.” *Id.*, 9:2-4. I understand that in response to the user's request, the service node generates a token or challenge code that is “sent over an authentication challenge network 28 to the personal unit.” *Id.*, 9:5-8. When a response code is generated by the personal unit, displayed to the user, and then input by the user into terminal 22, it is “compared to an expected response code,” that was “pre-stored or generated using the same algorithm and variables” in the service node or authentication center. *Id.*, 10:2-5. A POSITA would have understood that the new response code being compared is a new password because the “response code is to be unique to each transaction.” *Id.*, 7:34-35. A POSITA would have also understood that the new response code is a new password because it is being used to authenticate the user and allow access to the system. Furthermore, the response code would be recognized by a POSITA as

a new password because it is known by only two parties: the user and the authentication center.

114. I note that in combination, *Veneklase*'s authentication system would incorporate *Jonsson*'s teachings related to using an algorithm to create a new password (e.g., response code) following a user's request for a token (e.g., random code/challenge code).

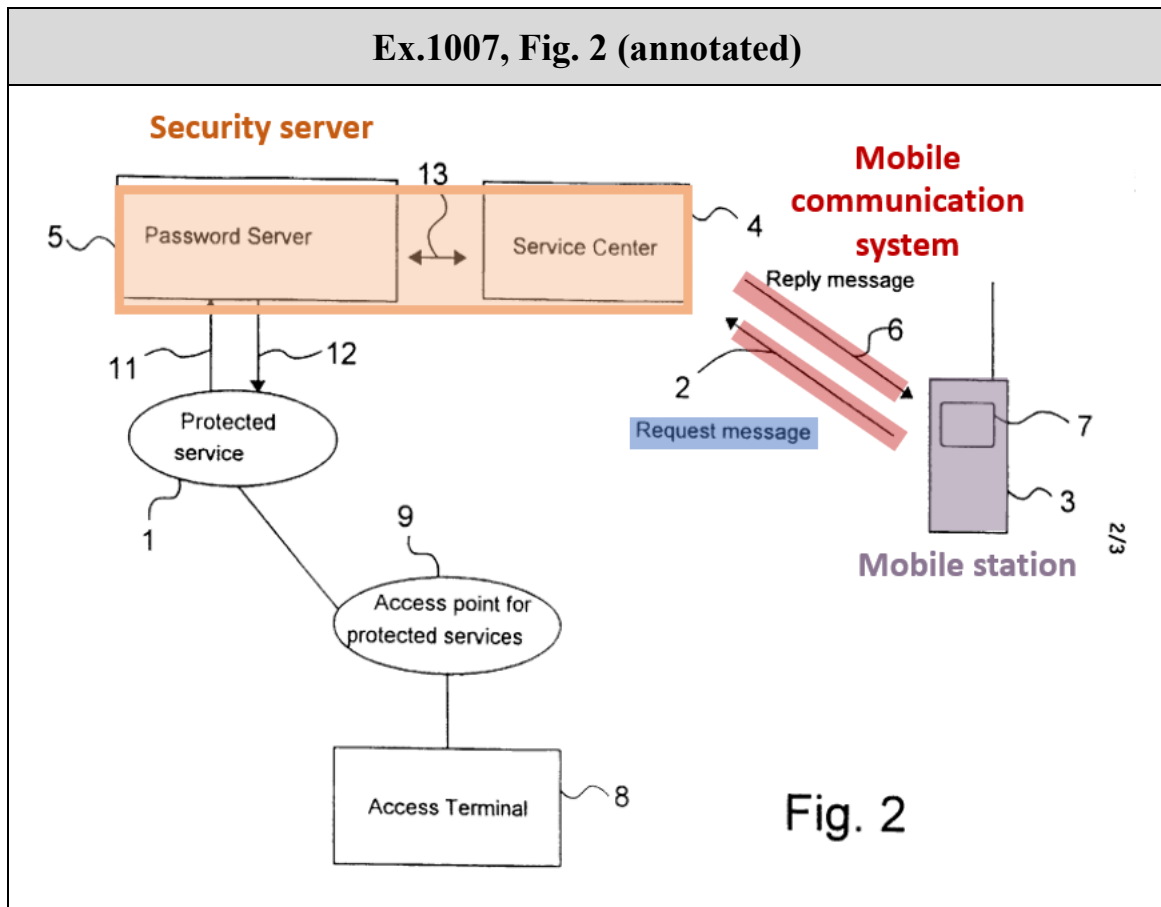
115. In my opinion, *Veneklase* in combination with *Jonsson* therefore teaches *wherein the communication module* (e.g., user/password check module) *is further configured to receive a request from the user for the token* (e.g., random code/challenge code), *and wherein the control module is further configured to create the new password in response to the request* (e.g., response code).

**D. Claim 7**

116. Claim 7 depends from claim 6, which I believe is obvious in view of *Veneklase* and *Jonsson* as I discussed in Section VII.C, and which I will avoid repeating here although my opinions as to claims 5 and 6 apply here as well since those elements are also in claim 7. Claim 7 adds: "*wherein the request is transmitted by the user through the personal communication device.*"

117. In my opinion, claim 7 is rendered obvious by *Veneklase* in view of *Jonsson* and *Sormunen*. Specifically, *Sormunen* discloses that in order to obtain a

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



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

119. *Sormunen*’s “paging service center 4 processes the incoming message and forms according to it a data transmission connection to a password server 5 and transmits the inquiry to it,” which “processes the message and forms a reply

message containing one or more passwords.” *Id.*, 6:20-24. *Sormunen* notes that “[t]he present invention can be applied especially in such telecommunication systems in which it is possible to transmit short messages...on the basis of a terminal key, such as a telephone number,” and that “[t]his quality is included in mobile communication systems” such as “a **cellular system, a paging system, and a mobile phone system.**” *Id.*, 4:30-5:8.

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

**E. A POSITA Would Have Been Motivated to Combine *Veneklase*, *Jonsson*, and *Sormunen***

121. I believe a POSITA would have been motivated to combine *Veneklase*, *Jonsson*, and *Sormunen* for a number of reasons.

122. As a threshold matter, I note that a POSITA would have appreciated that all references are within the same field of endeavor and address similar problems as each other and the '658 Patent. *See* Ex.1001, 1:7-11 (discussing systems for “authentication of users of secure systems and...system[s] through which user tokens required for user authentication are supplied through personal communication devices”). *Veneklase* discloses “computer security systems...which are adapted to grant an authorized individual access to a secured domain” by use of a pager. Ex.1005, Abstract (“). Like *Veneklase*, *Jonsson* discloses “[a]uthorization for a user to use a service is provided by a modified pager.” Ex.1006, Abstract. And *Sormunen* discloses a “method for obtaining at least one item of user specific data . . . at least partly by using paging or a short message service.” Ex.1007, Abstract.

123. I observe that all three references are particularly pertinent to another aspect of the '658 Patent's teachings of authenticating user access “using a device that many users already carry,” e.g., “a mobile phone or a pager.” Ex.1001, 1:56-59. *Veneklase* discloses the same solution of using a mobile device for

authentication. Ex.1005, 8:5-15. *Jonsson* likewise avoids the shortcomings of prior art systems “requir[ing] specially equipped, and often dedicated, terminals, which raises the cost and reduces the availability of the associated electronic service.” Ex.1006, 2:8-14. And *Sormunen* solves the same problem by transmitting authentication information to the user via a mobile network. Ex.1007, 4:30-5:8.

124. I believe a POSITA would have been motivated to combine the three references because such a combination would be commercially desirable and obvious to try. Indeed, *Sormunen* teaches the use of conventional mobile communication systems, e.g., the well-known GSM system. Ex.1007, 5:1-3. *Veneklase* likewise advocates for a “typical communications channels,” and further identifies several benefits of its invention, including that it is “relatively low-cost, but effective” and “very cost effective as it employs substantially ‘off the shelf’ and readily available components.” Ex.1005, 7:13, 7:17-24, 7:44-45. Additionally, *Jonsson* makes clear that its teachings can be implemented using conventional technology, including conventional mobile phones: “the capacity for performing the necessary calculations exists in conventional cellular telephones...allowing the present invention to be implemented through software.” Ex.1006, 7:24-31.

125. I observe that in view of *Veneklase*'s advantages of being "very cost effective" and "readily available," a POSITA would have been motivated to further modify *Veneklase* by implementing its system using a conventional cellular system (e.g., GSM), as taught by *Sormunen*, to make it widely accessible to mobile phone users. In my opinion, a POSITA would recognize that by doing so, the system in *Veneklase* would also benefit from the fast data speeds and security offered by widely deployed communications networks to allow for secure access to a service "almost immediately" after a request is sent. *See* Ex.1007, 5:12-18 (the "present invention enables very fast subscription," and "[a] further advantage of the fast data transmission is that...security may thus be improved"). Thus, it is my belief that a POSITA would have been motivated to combine *Veneklase*, *Jonsson*, and *Sormunen* in order to maximize the accessibility, performance, efficiencies, and security offered by the systems and methods disclosed in each reference.

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

the user will be able to learn of and use the token before the token expires. Indeed, instead of requesting a token from a computer terminal and sending it to a device that the user has potentially misplaced or cannot readily locate, the *Veneklase + Jonsson* system as modified by *Sormunen* would allow that user to simply request the token from a device they may already have at hand and are using. I believe this would enhance the user-friendliness and convenience of the system and provide desirable and marketable features. This modification would not sacrifice the security of the system because, as I discussed above, *Veneklase* discloses maintaining a master database that correlates the user's mobile number with other identifying and password information. The *Veneklase + Jonsson + Sormunen* system would therefore utilize *Veneklase*'s database to confirm that the request came from the appropriate phone number before providing any token in response. Indeed, in my opinion, a POSITA would have recognized that this combination would offer increased security over the *Veneklase + Jonsson* system by ensuring that tokens are only sent to devices already in the hands of the user at the time of the request, rather than to a device that may have been misplaced or even lost.

127. Additionally, a POSITA would have also recognized that personal communication devices, for example cellular phones, were becoming more available and less expensive. A POSITA would have also recognized that the availability of Short Message Service (SMS) enabled a cellular phone, through a

cellular phone network, to perform similar functions previously provided by a paging network. As discussed elsewhere, cell phones provided more features and had, e.g., richer user interfaces and more processing capacity, and configurability.

128. I also have one final point to offer on the extensive motivation that would have existed to combine these references. On that point, I believe a POSITA would have been motivated to combine these references because adding *Sormunen*'s token-request functionality merely applies known techniques to improve similar systems and devices. For example, *Sormunen* discloses that its token-request functionality could be implemented with the already-existing cellular system described in *Veneklase* and *Jonsson*. See Ex.1007, 4:30-5:8; Ex.1005, 6:37-44; Ex.1006, 5:27-35. In my opinion, a POSITA would have recognized that this implementation would merely involve applying known techniques to modify mobile phone software to allow a user to transmit a token request over a cellular system and to modify system software to receive and recognize that request. Indeed, a POSITA would have recognized that such an implementation could be readily achieved and work successfully without any modifications to any system, device hardware, or existing cellular systems.

129. Therefore, it is my opinion that a POSITA would have been motivated to modify, and would have had a reasonable expectation of success in modifying, *Veneklase*'s authentication system with *Jonsson*'s teachings related to its algorithm

and *Sormunen*'s teachings related to the transmission of token requests over a cellular network.

**VIII. MY OPINIONS AS TO CLAIM 2 IN CONSIDERATION OF  
VENEKLASE IN VIEW OF JONSSON, SORMUNEN, AND KAUFMAN**

130. Claim 2 depends from claim 1, which I believe for the reasons provided below to be rendered obvious by the combination of *Veneklase*, *Jonsson*, *Sormunen*, and *Kaufman*.

**A. Claim 1**

131. As I note in the chart below, and with the exception of limitation 1[b], claim 1 recites limitations analogous in scope to those of claim 5. For the corresponding sections referenced in the chart below, my opinions expressed in the corresponding section for limitations of claim 5 apply equally to the analogous limitations that appear in claim 1. For brevity, I am not going to repeat those opinions here again, but they of course apply equally here.

| <b>Claim 1<br/>Limitation</b> | <b>Corresponding Analogous<br/>Claim 5 Limitation(s)</b> | <b>Section(s) that Apply<br/>Equally Here</b> |
|-------------------------------|----------------------------------------------------------|-----------------------------------------------|
| 1[pre]                        | 5[pre], 5[e], 5[f]                                       | VII.A.1, VII.A.6, VII.A.7                     |
| 1[a]                          | 5[b], 5[e]                                               | VII.A.3, VII.A.6                              |
| 1[b]                          | <i>See Claim 7 and below</i>                             | VII.D                                         |
| 1[c]                          | 5[c]                                                     | VII.A.4                                       |
| 1[d]                          | 5[c]                                                     | VII.A.4                                       |

| Claim 1 Limitation | Corresponding Analogous Claim 5 Limitation(s) | Section(s) that Apply Equally Here |
|--------------------|-----------------------------------------------|------------------------------------|
| 1[e] <sup>7</sup>  | 5[f]                                          | VII.A.7                            |
| 1[f]               | 5[d]                                          | VII.A.5                            |
| 1[g]               | 5[e]                                          | VII.A.6                            |
| 1[h]               | 5[f]                                          | VII.A.7                            |

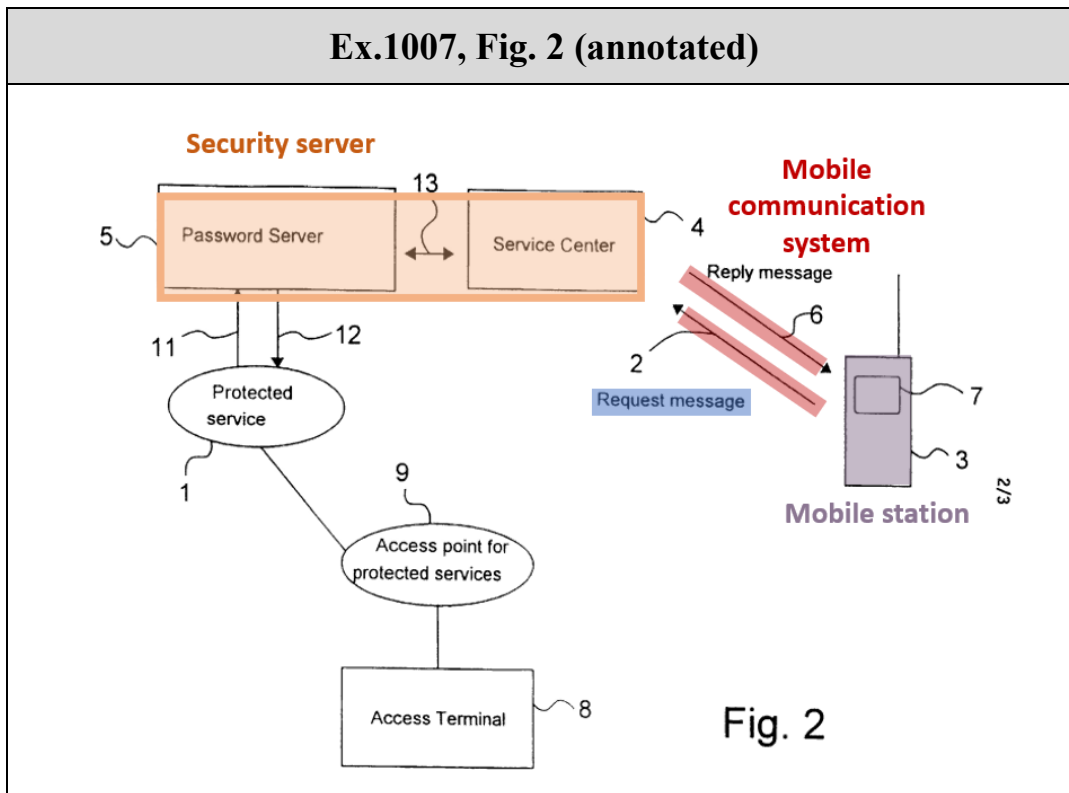
**1[b]— “receiving a request from the user for a token via the personal communication device, over the second network;”**

132. In my opinion, *Veneklase* in combination with *Jonsson* and *Sormunen* renders obvious this limitation. I observe that *Sormunen* discloses that in order to obtain a password or list of passwords, “**the user of the service sends a short message 2 from the paging terminal 3, such as a mobile station.**” Ex.1007, 5:35-38, Fig. 2. “[T]he short message 2 includes a **password request.**” *Id.*, 5:38-6:1.

---

<sup>7</sup> I understand the district court did not construe the “activating access” limitation in claim 1[e] the same as the “activates access” limitation in claim 5[f].

Regardless, under either of the two different constructions that I discussed above, this limitation is rendered obvious as I discussed above with respect to the section titled “Unified IPR Board Construction” in Section VII.A.7.



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

134. I understand that *Sormunen*’s system can be utilized in “telecommunication systems in which it is possible to transmit short messages,” for example, “mobile communication systems includ[ing] [] a **cellular system, a paging system, and a mobile phone system.**” Ex.1007, 4:30-5:8; *see also id.*, claim 11.

135. I believe a POSITA would have understood that the request for a password issued through *Sormunen*'s mobile request system would be for a token (e.g., randomly generated challenge code) in accordance with the combined *Veneklase* and *Jonsson* system that I described above with respect to claims 5-7.

136. In my opinion, *Veneklase* in combination with *Jonsson* and *Sormunen* discloses *receiving a request* (e.g., a password request) *from the user for a token* (e.g., randomly generated challenge code) *via the personal communication device* (e.g., receiver unit/paging terminal), *over the second network* (e.g., cellular network which differs from the first network comprising secure computer network or security server). As noted previously above, I provided further analysis concerning claim 7 (which recites aspects similar to 1[b]), and the analysis as to claim 7 applies equally to my opinions as to 1[b].

## **B. Claim 2**

137. I observe that claim 2 depends from claim 1, and adds “*wherein the new password is generated by concatenating the token and the passcode.*” In my opinion, *Veneklase* in view of *Jonsson*, *Sormunen*, and *Kaufman* renders this limitation obvious.

138. As I briefly summarized above, *Kaufman* discloses a system utilizing a password and a token, and that “workstation 516 **computes a ‘transmission code’ based upon the password and the token.** Ex.1008, 9:39-42. *Kaufman*'s

transmission code is calculated by using a first ‘hashing algorithm.’” *Id.* I understand *Kaufman*’s “hashing algorithm” is “a one-way routine for transmuting multiple input data items, [that] **concatenat[es] selected items of the input data** and perform[s] a ‘hashing equation’ upon one or more items of the input data, in a specified order.” *Id.*, 9:43-46. I note that the disclosed “hashing equation” can “include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence.” *Id.*, 9:47-51.

139. I observe that *Kaufman* discloses different hashing algorithms that may be used to concatenate tokens and passcodes:

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

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

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

*Id.*, 9:65-10:5. As the table above shows, *Kaufman* thus teaches concatenating the password onto the token, hashing the concatenation, and then again hashing the resulting hash value (1.1), concatenating the token onto the password and then hashing the concatenation (1.2), and also concatenating the password onto the token and then hashing the concatenation. Notably, the claim does not specify in which order the concatenation must occur (whether the token is concatenated onto the password, or vice versa) and, in any event, *Kaufman* discloses concatenating in any order. The claim also does not preclude the use of a hashing algorithm after concatenating the values, so *Kaufman* is directly on point in terms of teaching what claim 2 recites.

140. As further confirmation, I also observe here that a POSITA would have appreciated that the modified password of *Kaufman* that can be concatenated onto the token to form a concatenation (1.1 and 1.3 in the table of *Kaufman* I was just discussing) is similar to the concatenation operation disclosed in the '658 Patent. See Ex.1001, 4:52-53, Figs. 2A-2D. Indeed, the '658 Patent teaches “the

user 108 can combine a valid memorized passcode of ‘abcd’ with a valid token of ‘1234’ to form a valid password of ‘abcd1234.’” *Id.* Therefore, a POSITA would have understood that *Kaufman* discloses that “the new password [*Jonsson* response code] is generated by concatenating [the concatenating operation that occurs prior to application of *Kaufman*’s hashing algorithm] the token [*Jonsson*’s received challenge code] and the passcode [*Jonsson*’s PIN].”

141. It is thus my opinion that *Veneklase* in combination with *Jonsson*, *Sormunen*, and *Kaufman* discloses *wherein the new password* (e.g., transmission code) *is generated by concatenating the token and the passcode.*

C. **A POSITA Would Have Been Motivated to Combine *Veneklase*, *Jonsson*, *Sormunen*, and *Kaufman***

142. In my opinion, a POSITA would have had ample motivation to further combine the teachings of the combined system of *Veneklase*, *Jonsson*, and *Sormunen* with *Kaufman* as well.

143. Preliminarily, as to analogous art, and just like the other three references, I note that a POSITA would have appreciated that *Kaufman* is analogous art that is within the same field of endeavor and addresses the same problems as that of the ’658 Patent. The ’658 Patent identifies the claimed invention as one which relates “generally to the authentication of user of secure systems and, more particularly, . . . to a system through which user tokens required

for user authentication are supplied through personal communication devices such as mobile telephones and pagers.” Ex.1001, 1:7-11. Like the ’658 Patent, *Kaufman* discloses a method “by which an authentication server in a distributed computing system may transmit an authentication ‘ticket’ to a user, authorizing access by the user to specified system resources.” Ex.1008, 1:25-28; *see also* Ex.1001, 1:7-11.

144. Additionally, I understand that *Kaufman* addresses similar problems to that identified by the ’658 Patent. The ’658 Patent notes that “passwords created by users are often combinations of words and names, which are easy to remember but also easily guessed” and “guessing passwords is a frequent technique used by ‘hackers’ to break into systems.” Ex.1001, 1:28-31. Similarly, *Kaufman* explains that “[a]n authentication system based solely on passwords and user names is open to attack by would-be intruders,” that “user names often are not difficult for unauthorized persons to determine,” and that “when users are allowed to select their own passwords, they tend to choose passwords that are easily remembered...[and] can be easily guessed as well.” Ex.1008, 2:8-15.

145. Like the ’658 Patent, *Kaufman* discloses leveraging the “SecurID product” as a token generator to maintain security while enabling access to remotely stored information. *Compare* Ex.1008, 8:57-60 (“The token generators

520, 522 may, for example, comprise units such as SecurID™.”), with Ex.1001, 1:56-59; see also Sections VII.B, VII.E.

146. Having established *Kaufman* is analogous art to the '658 Patent, I also believe a POSITA would have been motivated to implement *Kaufman*'s teachings in combination with *Veneklase*, *Jonsson*, and *Sormunen* to achieve the benefits that *Kaufman* provides. For instance, I understand that *Veneklase* discusses potential drawbacks associated with “prior encryption techniques,” for example that they are “relatively costly and complicated and require one or more known ‘encryption keys’ which are in constant exchange between users” and are thus “susceptible to theft and/or inadvertent disclosure.” Ex.1005, 2:37-48. Part of *Veneklase*'s solution to this (and other) identified issue(s), is to rely on individualized passwords that are known to the user, as well as sending a randomly generated token, as discussed above at length.

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

10:17. Thus, a POSITA seeking to build *Veneklase*'s system would have had a motivation to achieve the security goals that *Veneklase* highlights and this would have led the POSITA to consult analogous references like *Kaufman*. In so doing, the POSITA would have encountered the concatenation operation and associated hashing algorithm and would have been motivated to implement that in the combined system (or at least try doing so) to achieve the enhanced security goals that *Veneklase* emphasizes.

148. In my opinion, a POSITA who is looking to maximize the benefits of *Veneklase*'s invention would have been motivated to consult other analogous references to do so, and would have then had a motivation to implement *Kaufman*'s disclosed concatenation and "cryptographically secure hashing algorithm" (Ex.1008, 7:2-5) in order to add an additional layer of security, which is the primary problem to be solved by *Veneklase*'s system.

149. I believe a POSITA would be further motivated to implement *Kaufman*'s "hashing algorithm" into *Veneklase*'s system because the combination merely uses a known technique to improve similar devices in a similar way. For example, I believe a POSITA would have been motivated to utilize the "hashing algorithm" in *Kaufman* (including the concatenation operation that occurs before the hashing algorithm is applied) in the system of *Veneklase* because it would have been a simple replacement or additional process to apply in connection with

generating *Veneklase*'s "random number code." I also believe a POSITA would have had a reasonable expectation of success in modifying these systems by combining them as the implementation of an additional algorithm for use in an authentication system is a simple and commonplace exercise for a POSITA.

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

**IX. MY OPINIONS AS TO CLAIM 7 IN CONSIDERATION OF KEW IN VIEW OF SORMUNEN**

151. Claim 7, through its dependencies, includes the limitations of claim 6 and claim 5, and in my opinion the combination of *Kew* and *Sormunen* renders all of the limitations of claim 7 obvious.

**A. My Opinions as to Aspects of Claim 7 that are Inherited from Claim 5**

**1. 5[pre]**

152. As I mentioned above, I have been informed that claim preambles are generally not limiting. In any case, to the extent the preamble is limiting here, I believe that *Kew* discloses an authentication system. *See* Ex.1009, Abstract, 1:3-5, 1:20-2:23, 7:10-35, Fig. 1.

Ex.1009, Fig. 1

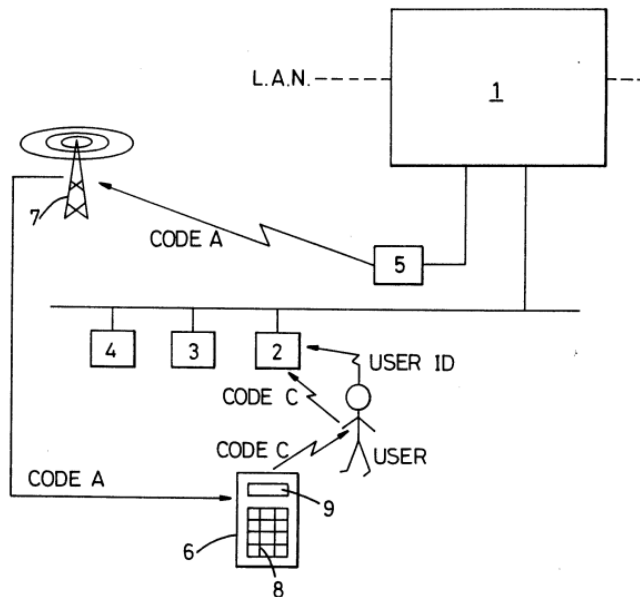


Fig. 1

2. 5[a]

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

**Ex.1009, Fig. 1 (annotated)**

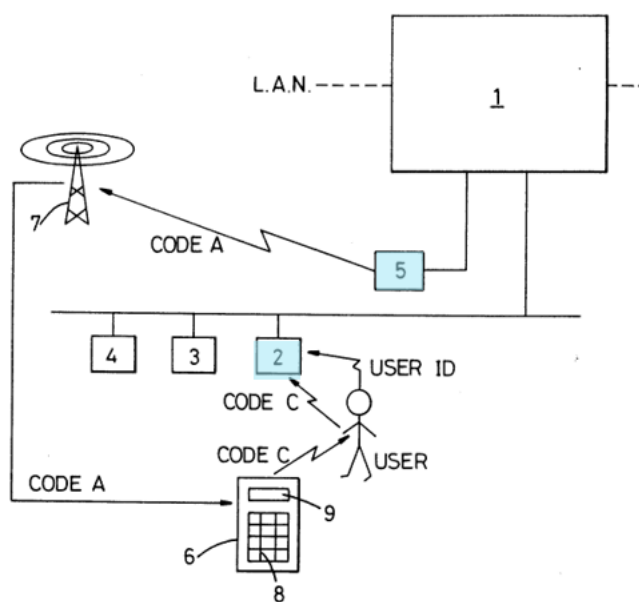


Fig. 1

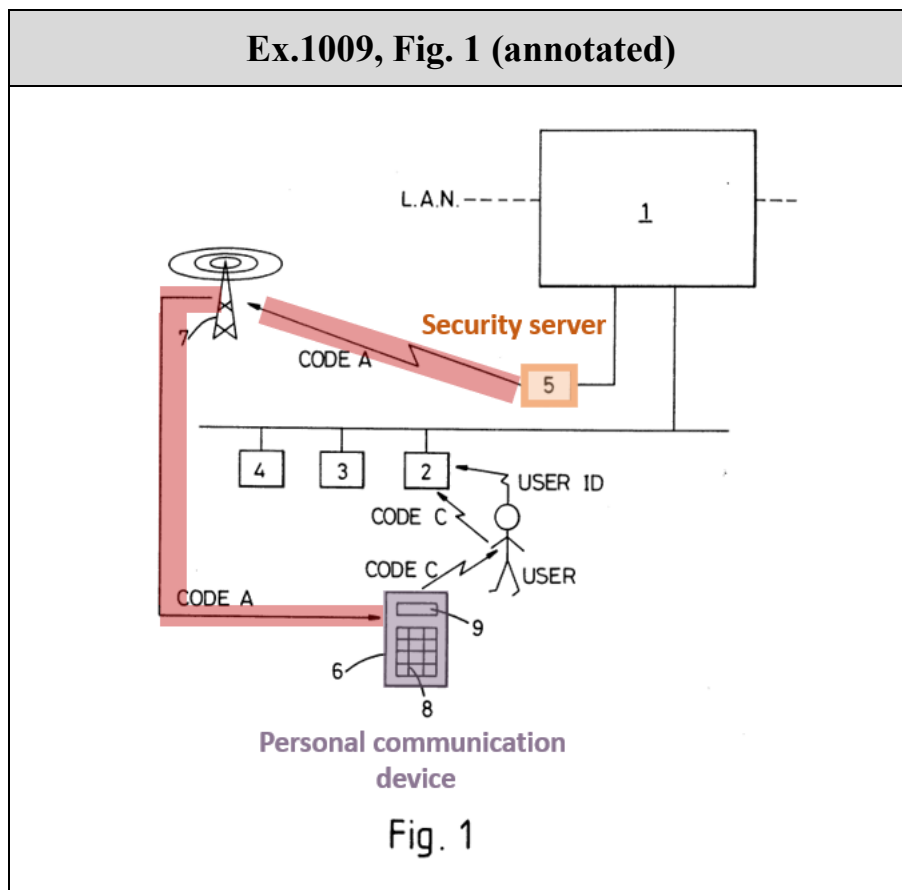
154. In my opinion, a POSITA would have understood *Kew*'s disclosure to teach that both computer terminal 2 and security server 5 contain a central processing unit. To perform its server function, security server 5 would have necessarily included a computer processor. Likewise, to operate as a terminal and interface with a user, computer terminal 2 necessarily would have included a computer processor.

155. It is therefore my opinion that *Kew* teaches *a computer processor* (e.g., central processing unit).

### 3. 5[b]

156. In my opinion, *Kew*, alone or in combination with *Sormunen*, teaches or renders obvious this limitation. *Kew* discloses that “security server 5 includes a **database of all authori[z]ed users and their authori[z]ed receiver units 6, and identifies the corresponding identity code for the appropriate receiver unit 6,**” which could be a personal communication device such as a pager. Ex.1009, 8:2-5, 8:12-23.

157. *Kew* additionally teaches *a personal communication device configured to communicate over a cell phone network with the user authentication system*. For example, *Kew* discloses that the receiver unit 6 can be a personal communication device, such as a pager. *See, e.g.*, Ex.1009, 8:12-23. I note that *Kew* also discloses that “security server 5 also transmits ... to a paging system 7,” and that transmitted information is then “broadcast by the paging system 7, typically using a radiofrequency transmitter,...similar to conventional paging systems.” Ex.1009, 8:13-19. “[T]he receiver unit 6 will use the identifier to pick out the appropriate signal.” *Id.*, 8:20-21.



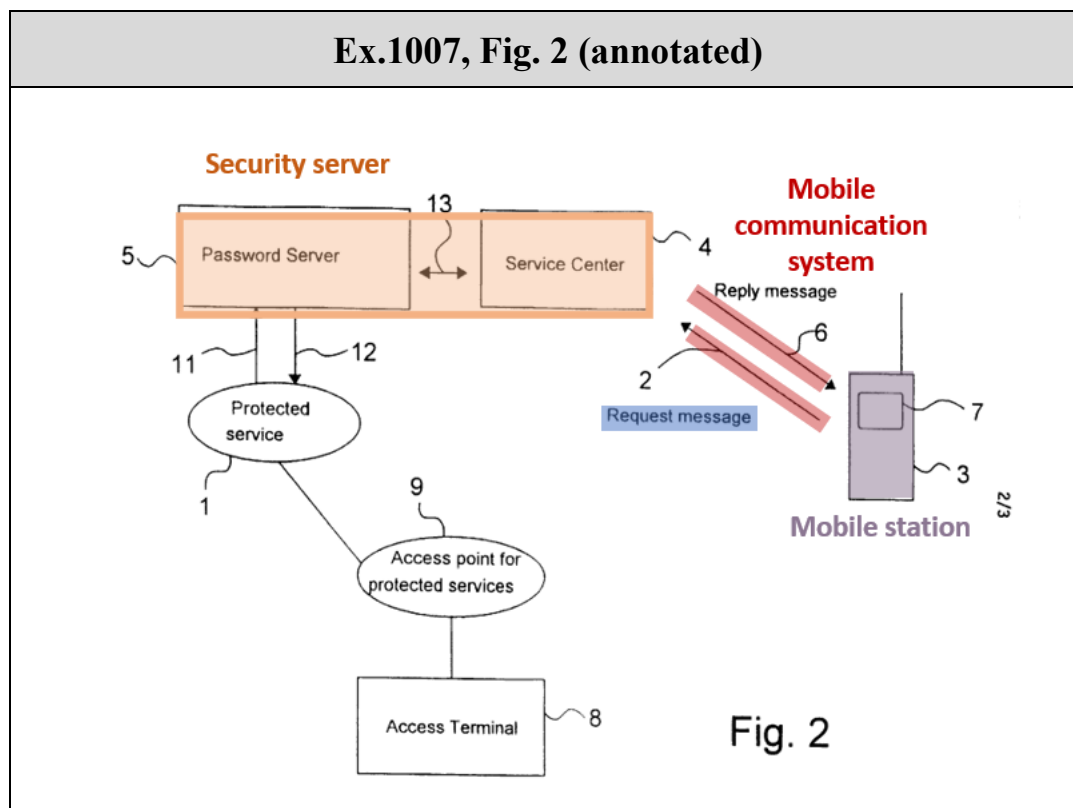
158. In my opinion, a POSITA would have understood that *Kew*'s communication channel is analogous to the networks disclosed in the '658 Patent, which include cellular and pager networks. See Ex.1001, 5:34-40 ("The communication module 118 forwards tokens 156 to a text messaging service provider 104,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

159. To the extent PO asserts that *Kew*'s pager network does not disclose the claimed cell phone network, I believe a POSITA would have found it obvious to implement the authentication system of *Kew* using a cell phone network. I

observe that *Kew* explicitly contemplates that the device 6 and the security server 5 communicate via “radiofrequency transmitter[s].” Ex.1009, 8:12-23. While the example provided in *Kew* is a pager system, I believe a POSITA would have found it obvious to use a cell phone network, which is another type of communication that utilizes radiofrequency transmission. In my opinion, it would have also been obvious to use a cell phone network to send *Kew*’s random code (Code A) because doing so would have made the system available to even more users in more locations, which is one of the intentions of the reference. *Id.*; *see also* Ex.1009, 4:8-12, 8:15-23, 13:29-14:6. I note that it would also have been obvious because cell phones were preferred to pagers during the relevant time period for multiple reasons, such as for their larger screens, buttons, and user interfaces. Alternatively, a cellular network could have been used to communicate with a pager for at least the reasons above and also because it would have been obvious to try due to the finite number of networks available at the time to communicate with a mobile pager. It is my understanding that a POSITA would have had a reasonable expectation of success in modifying *Kew*’s authentication system to use a cellular network instead of a pager network because they operate similarly, many times using the same protocols, and would only involve swapping out devices and/or making certain software configuration changes, all of which are routine and common tasks for a POSITA.

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

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



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

163. In my opinion, *Kew* alone, and also in combination with *Sormunen*, discloses this limitation.

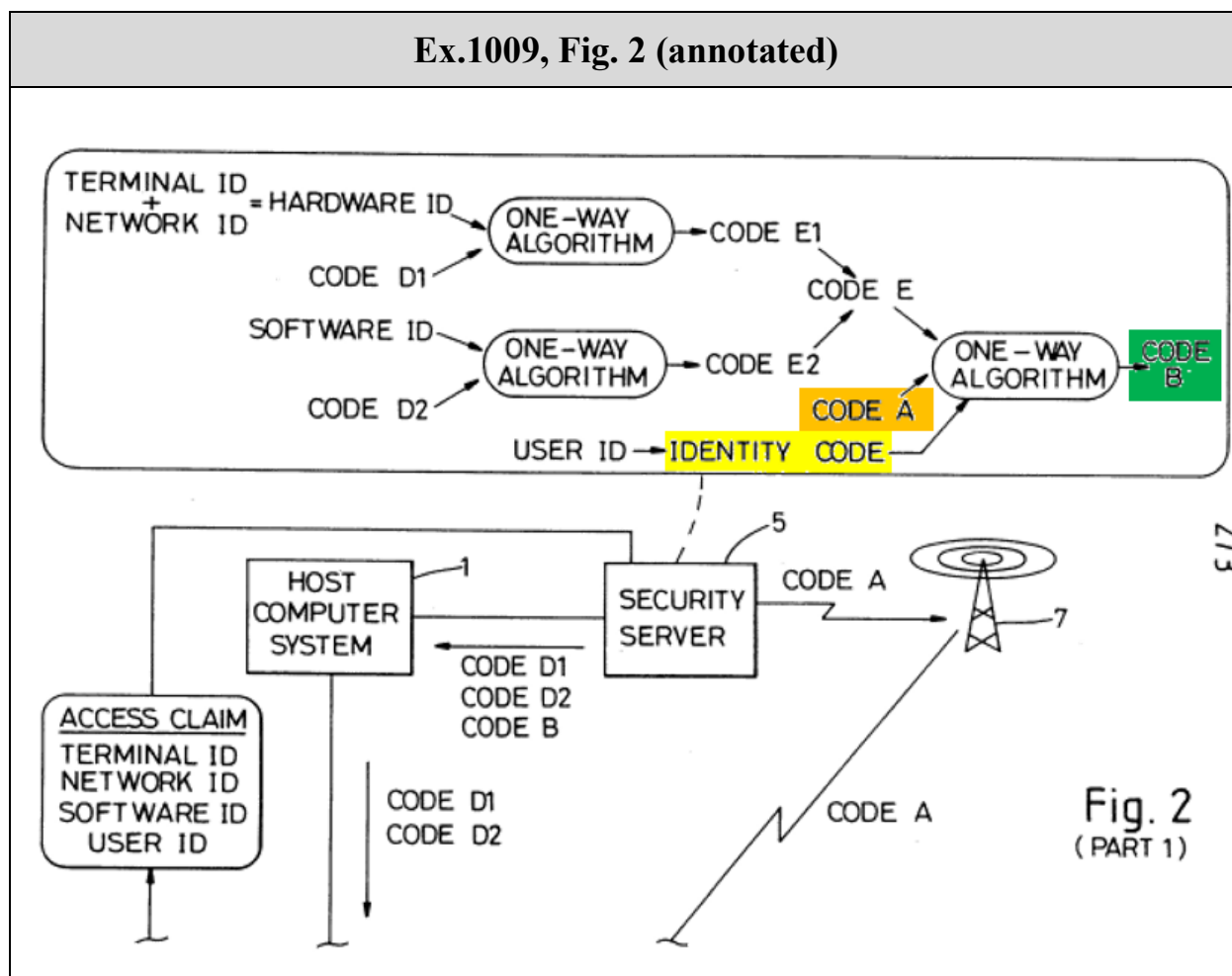
#### 4. 5[c]

164. In my opinion, *Kew* teaches or renders obvious this limitation. *Kew* discloses that after the user enters his user identification code, “the security server 5 then **generates a random code (Code A)** and subjects this number to an encryption using the same one-way algorithm as is stored in the user’s receiver 6 together with the corresponding **identity code**” to create a “**transformed code (Code B)**.” Ex.1009, 8:5-10. *Kew* further discloses that “the security server 5 also

transmits the random code [(Code A)] to a paging system 7 along with an identifier or identifying tag which can be recognized by the receiver unit 6.” *Id.*, 8:12-15.

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

Ex.1009, Fig. 2 (annotated)



166. Because Code A is randomly generated by security server 5, it is my understanding that Code A is not known to the user prior to it being sent to the receiver unit. The user's identity code, on the other hand, "should preferably be treated by the user as a secret code" and "is thus comparable with a personal identification number (PIN)," and is therefore known to the user beforehand.

Ex.1009, 3:8-12, 7:36-8:2.

167. *Kew* additionally discloses that "terminal 2, at the behest of the security server 5 prompts the user to input the transformed Code C displayed by

the receiver unit 6” and that “security server 5 [then] **compares the input Code C with the transformed code, Code B**, it produced by encryption of the random code, Code A.” Ex.1009, 9:5-11. Therefore, I believe a POSITA would have understood that *Kew*’s security server is setting transformed Code B—that the security server created by encryption of random Code A—to be the new **password**, *i.e.*, the password against which the user’s input code (Code C) is compared.

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

## 5. 5[d]

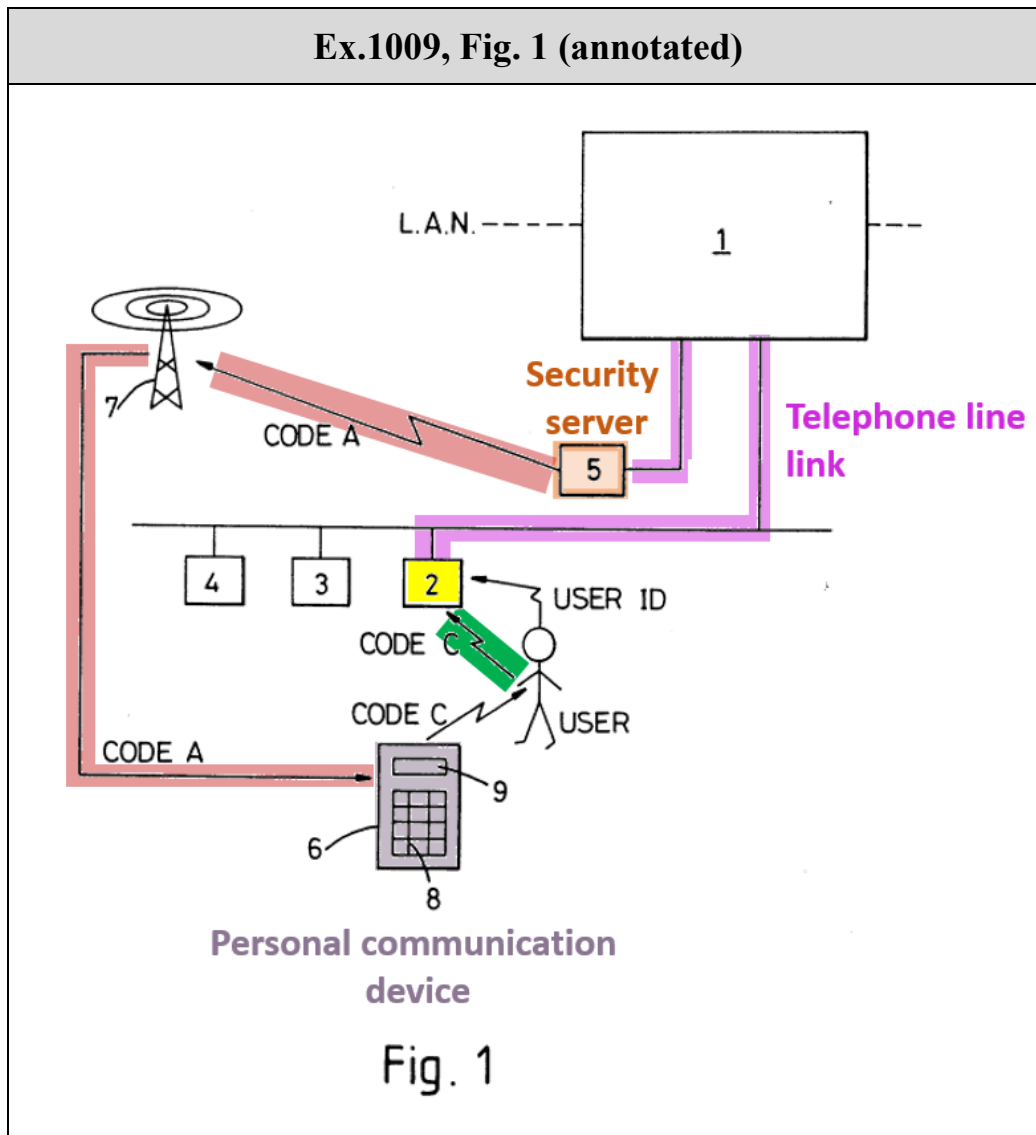
169. In my opinion, *Kew* teaches or renders obvious this limitation. *Kew* discloses that its system includes “transmitting Code A [the randomly generated token] via a paging system, to a receiver held by the user.” Ex.1009, 1:31-32. As I discussed in Section IX.A.3, “the security server 5 also transmits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

broadcast by the paging system 7, typically using a radiofrequency transmitter, in a fashion similar to conventional paging systems.” *Id.*, 8:12-19. Also, as I discussed in Section IX.A.3, *Kew*’s communication channel is akin to the cellular and pager networks disclosed in the ’658 Patent, and at the very least, a POSITA would have found it obvious to use a cellular network for the transmission of *Kew*’s randomly generated token to a personal communication device (I explained above why this is the case or, at a minimum, why it would have been obvious to modify *Kew* to make use of the cellular phone and associated cellular network taught by *Sormunen*). Indeed, the ’658 Patent discloses an embodiment in which “the communication module 118 is a phone dialer 622, the personal communication device 106 is a pager 624, and the text messaging service provider is a paging service 626.” Ex.1001, 10:31-34. I note that this is very similar to what is disclosed in *Kew*. Thus, it is my understanding that the “cell phone network” claimed in the ’658 Patent also includes the pager network, as disclosed in *Kew*.

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

6. 5[e]

171. In my opinion, *Kew* teaches or renders obvious this limitation. It is my understanding that *Kew* discloses *an authentication module* (e.g., a portion of security server 5) *configured to receive the password from the user through a secure computer network* (e.g., user is prompted by server 5 to input Code C). Specifically, *Kew* discloses that “the receiver unit 6...uses the received random number and the identity code stored in its own EPROM to produce a transformed code (Code C),” which is “then displayed to the user.” Ex.1009, 8:33-9:3. “[T]he 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.” *Id.*, 9:5-7. This information is entered into a remote terminal 2, which I observe is connected to the host computer system 1 “via a telephone line link.” *Id.*, 7:10-14, Fig. 1.



172. A POSITA would have understood that this connection, which is different from the pager network connecting the system to the personal receiver device (and is also different from the modified system making use of a cell network in place of a pager network), is secure at least because the connection requires that a user verify their identity. For example, *Kew* discloses “a computer security system...for preventing unauthorized access to a host computer system.”

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

173. In my opinion, *Kew* teaches *an authentication module* (e.g., a portion of security server 5) *configured to receive the password from the user through a secure computer network* (e.g., by prompting the user to input Code C), *said secure computer network being different from the cell phone network* (e.g., a telephone line link).

## 7. 5[f]

174. In my opinion, *Kew* discloses or renders obvious this limitation.

175. ***Activates Access – Unified IPR Board Construction.*** As I discussed above, I understand that the Board in the Unified IPR rejected Petitioner’s arguments and stated that “Claim 5 ... does not require that the account be activated in response to creation of the password.” Ex.1013 (Paper 9 at 24). Here again, the adoption (or not) of this construction makes no difference to my opinions as the references I rely on here teach the claim under either the Board’s

construction (discussed in the next sentences) or the district court’s construction (discussed below). *Kew* discloses *wherein the authentication module* (e.g., a portion of security server 5) *activates access to the account in response to the password* (e.g., if Code B and Code C match, access to host system 1 is permitted). Specifically, I understand *Kew* discloses that once the user has input the transformed Code C, **“the security server 5 compares the input Code C with the transformed code, Code B”** and **“[i]f Code B and Code C are identical, access to the host system 1 is permitted.”** Ex.1009, 9:5-11, 1:36-2:3.

176. *Activates Access – District Court’s Construction.* To the extent the Board here adopts Judge Payne’s construction (Ex.1011, 16)—which, as discussed above is “activates access to the account in response to the creation of the password” (Ex.1011, 16), *Kew* renders obvious this limitation. A POSITA would have recognized that when *Kew*’s transformed code (Code B) is created, the “database of all authori[z]ed users” is updated to associate Code B with the appropriate user and devices. Ex.1009., 7:34-8:10. The POSITA would have also recognized, or at least found it obvious, that this password creation and association in the database would activate the user account such that—after the creation of Code B—it could be readily accessed by a user. For additional security, I note that it would have further been obvious to allow for the account to be activated so that it could be accessed by inputting Code C on the personal communication device.

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

178. Additionally, it is my opinion that *Kew*'s system *deactivates the account within a predetermined amount of time after activating the account (e.g., enabled for a predetermined period), such that said account is not accessible through any password via the secure computer network (e.g., an unauthorized user cannot gain access to the system even if he has possession of the receiver and knows the user identification code)*. Specifically, *Kew* discloses that **"the receiver can only be enabled for a predetermined period to permit it to transform the received Code A to the transformed Code C by input of a second user identification code by the user."** Ex.1009, 3:14-17. In other words, a user only has a certain "predetermined period" to input the code required for access to the system. After that predetermined period of time, **"an unauthori[z]ed user cannot gain access to the system** even if he has possession of the receiver and knows the user identification code without knowledge of the second identification or activation code." *Id.*, 3:19-23. By only enabling the transformation of received

Code A to transformed Code C, which requires the input of a user identification code, *Kew* disables a user's access to the system after the predetermined time period.

179. I understand *Kew* further discloses that after the receiver device uses the received random number and the identity code to produce the transformed Code C, “[t]his **transformed Code C is then displayed to the user on a display means 9... for a predetermined length of time such as five minutes.**” Ex.1009, 8:33-9:3. A POSITA would have understood that by only displaying the transformed Code C that is required for system access for a predetermined period of time, *Kew* deactivates the account by not allowing access to the account via any password. I observe that once the predetermined period of time has run, the display is no longer visible, and the user would have to reactivate the account by starting the process over and having the system send a new randomly generated Code A.

180. I observe that *Kew*'s teaching is nearly identical to the '658 Patent's description. Indeed, I understand that the '658 Patent discloses in Figure 5 that the “user can access secure system by logging in using token” in step 516, but if the “token expires” in step 518, it “deactivate[s] user account in user database.” *See* Ex.1001, Fig. 5, 9:61-64 (“At a step 520, upon expiration of the token 156, the control module 402 deactivates the user account in the user database 114.”).

181. In my opinion, *Kew* teaches *wherein the user has an account on the secure computer network* (e.g., the user is listed as an authorized user in security server 5's database), *wherein the authentication module* (e.g., a portion of security server 5) *activates access to the account in response to the password* (e.g., if Code B and Code C are identical, access to the host system 1 is permitted) *and deactivates the account within a predetermined amount of time after activating the account* (e.g., enabled for a predetermined period), *such that said account is not accessible through any password via the secure computer network* (e.g., an unauthorized user cannot gain access to the system even if he has possession of the receiver and knows the user identification code).

**B. Claim 6**

182. Claim 6 depends from claim 5, which I believe is obvious in view of *Kew* and *Sormunen* as I discussed above in Section IX.A incorporated herein.

183. In my opinion, *Kew* teaches or renders obvious this limitation. *Kew* discloses that “[w]hen the user seeks access to the host system 1 via the terminal 2, he enters his user identification code.” Ex.1009, 7:34-35. Upon receiving the user identification code, “security server 5 then generates a random code (Code A) and subjects this number to an encryption using the same one-way algorithm as is stored in the user’s receiver 6 together with the corresponding identity code.” *Id.*, 8:5-10. In doing so, “transformed code (Code B) is produced.” *Id.* Therefore, a

POSITA would have understood that the user's submission of his user identification code serves as a request for the token (e.g., random Code A) to be sent to their personal receiver device and the security server also creates the new password (e.g., transformed Code B) in response to the request.

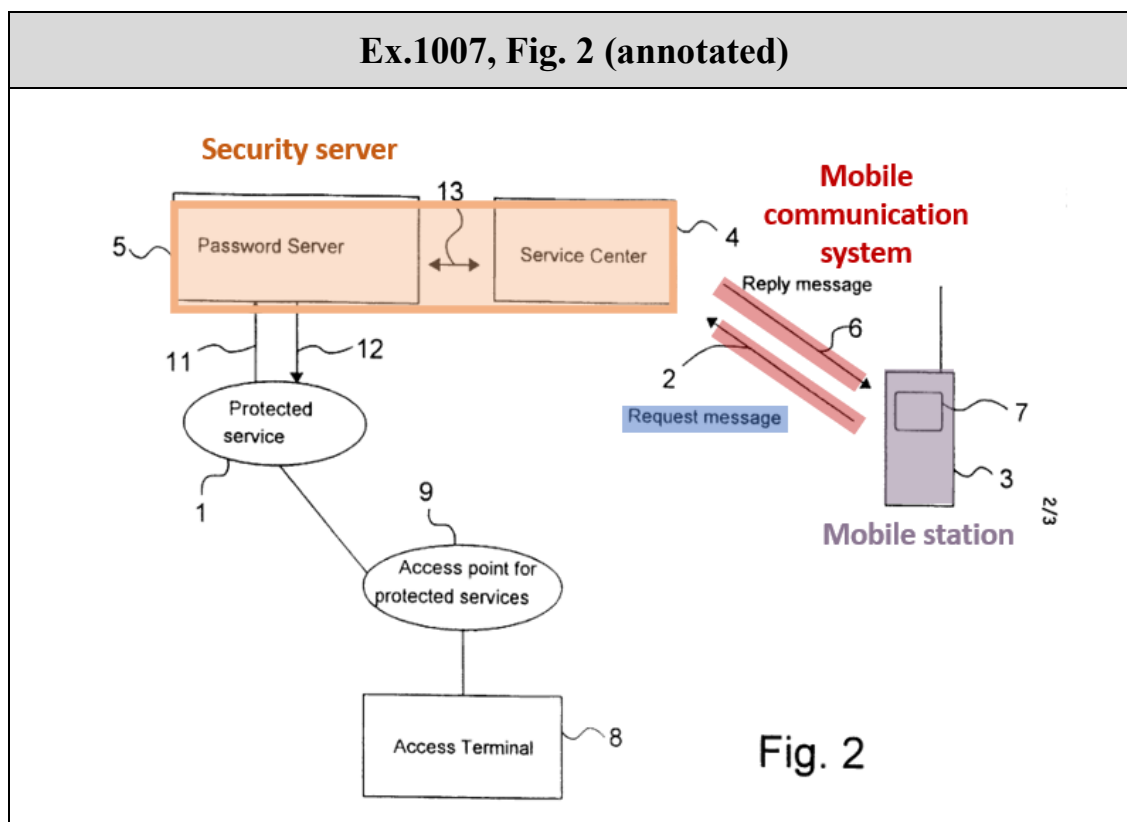
184. In my opinion, *Kew* teaches *wherein the communication module is further configured to receive a request from the user for the token* (e.g., receives a communication that leads to the creation of random Code A), *and wherein the control module is further configured to create the new password in response to the request* (e.g., transformed Code B is produced in response).

**C. Claim 7**

185. Claim 7 depends from claim 6, which I believe is obvious in view of *Kew* and *Sormunen* as I discussed above, and which applies here but is not repeated for brevity. Claim 7 adds: “wherein the request is transmitted by the user through the personal communication device.”

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

Ex.1007, Fig. 2 (annotated)



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

188. Next, it is my understanding that upon receiving the password request 2, *Sormunen*’s “paging service center 4 processes the incoming message and forms according to it a data transmission connection to a password server 5 and transmits the inquiry to it,” which “processes the message and forms a reply message containing one or more passwords.” *Id.*, 6:20-24. *Sormunen* notes that “[t]he present invention can be applied especially in such telecommunication systems in

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

189. In my opinion, *Kew* in combination with *Sormunen* discloses *wherein the request* (e.g., a password request) *is transmitted by the user through the personal communication device* (e.g., receiver unit, which can be a cellular phone in the modified *Kew-Sormunen* system).

**D. A POSITA Would Have Been Motivated to Combine *Kew* and *Sormunen***

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

191. Touching on the analogous nature of the references, I observe here that *Kew* and *Sormunen* are analogous art because they are in the same field of endeavor as the ’658 Patent. *Compare* Ex.1001, 1:7-11 (’658 Patent “relates generally to the authentication of user of secure systems and...to a system through which user tokens required for user authentication are supplied through personal

communication devices such as mobile telephones and pagers”) *with* Ex.1009, Abstract (“method of preventing unauthori[z]ed access to a host computer system...Code A is transmitted via a paging system (7), to a receiver (6) held by the user”), *and* Ex.1007, Abstract (“method for obtaining at least one item of user specific data...at least partly by using paging or a short message service”). In addition, I understand that both references are at least reasonably pertinent to another aspect of the ’658 Patent, namely, authenticating user access using a mobile phone or pager. Ex.1001, 1:56-59. *Kew* solves the same problem by using a generated random code sent “in a fashion similar to conventional paging systems.” *See, e.g.*, Ex.1009, 8:15-19. Similarly, *Sormunen* solves that problem by sending authentication information to the user via a mobile network. *See* Ex.1007, 4:30-5:8.

192. Turning to my opinions as to motivation, the motivations are numerous. For one, a POSITA would have been motivated to combine *Kew* with *Sormunen* in order to broaden access to the invention disclosed in *Kew* and access the benefits disclosed in *Sormunen*. *Kew* teaches a system in which a random code can be sent from a security server to a receiver unit via “conventional paging systems.” *See, e.g.*, Ex.1009, 8:12-23. *Sormunen* discloses a similar authentication system that allows a paging device to communicate with the authentication system via a cellular network, such as the well-known GSM system.

*See, e.g., Ex.1007, 4:30-5:8.* A POSITA would have been motivated to make such a combination because it would have allowed *Kew*'s authentication system to operate on the well-known and ubiquitous GSM system. Furthermore, I believe a POSITA would have been motivated to make such a combination because implementing *Kew*'s authentication system on *Sormunen*'s cellular network would allow for two-way communication between the receiver unit and the security server, and thus allow the user to request a random code via the receiver unit, as well as the terminal, which is precisely what is disclosed in *Sormunen*. *Ex.1007, 7:34-35.* Indeed, I understand a POSITA would recognize that by implementing *Kew*'s authentication system on the widely available GSM system disclosed in *Sormunen*, *Kew*'s system would obtain *Sormunen*'s benefits of allowing for secure access to a service "almost immediately" after a request is sent. *Ex.1007, 5:12-18* (the "present invention enables very fast subscription," and "[a] further advantage of the fast data transmission is that...security may thus be improved").

193. A POSITA would have also recognized that, in addition to broadening access to the system in *Kew*, adding *Sormunen*'s functionality for a user to remotely request a token, for example through *Sormunen*'s mobile device, would increase efficiency and add desired features to *Kew*'s system. For instance, if a user attempts to access the system disclosed in *Kew* but is unable to locate the token or the token expires, the user would have to initiate the initial request

through the remote terminal once again. By modifying the system in *Kew* with *Sormunen*, the user would be able to directly request the token from a mobile device already in their hands. I understand this would improve user-friendliness of the system and provide desirable and marketable features without compromising security. The combined system of *Kew* and *Sormunen* would implement *Kew*'s database to confirm that a token request came from the appropriate user. *See* Ex.1009, 8:2-5. A POSITA would have recognized that this combination would offer increased security by ensuring that tokens are only sent to devices already in the hands of the user at the time of the request, rather than to a device that may have been misplaced or even lost.

194. And the motivations do not stop there. I also understand that *Kew* explicitly provides a teaching, suggestion, and motivation for combining it with an authentication system that operates on other types of networks, such as those taught in *Sormunen*, because it explicitly discloses the use of a radiofrequency transmitter (thereby motivating a POSITA building out or attempting to build out *Kew*'s system to seek out all devices and networks compatible with that type of transmitter to expand market size and consumer appeal), which is also used in other systems, such as the GSM network. *See, e.g.*, Ex.1009, 8:15-19. Thus, I believe a POSITA would have been motivated to use *Kew*'s authentication system

in conjunction with receiver units that can operate on a cellular network, such as that described in *Sormunen*, to provide additional flexibility and features.

195. Moreover, I believe a POSITA would have further been motivated to combine *Kew* and *Sormunen* and had a reasonable expectation of success because the combination uses a known technique to improve similar devices in the same way. For example, I believe a POSITA would have been motivated to utilize the cellular network functionality of *Sormunen* in *Kew*'s system because it would have been used in the same way—e.g., to allow communication between a mobile device unit and a central server. I understand *Kew* discloses the use of radiofrequency transmitters operating via conventional systems (e.g., paging systems), so it would have been obvious for a POSITA to combine it with *Sormunen* (or at least try to do so given the finite number of network options and the ease with which a POSITA could have tried to build a system compatible with different network types, including pager and cellular networks from the relevant time period), which teaches that such a system can operate on paging systems as well as cellular systems and mobile systems. *See*, e.g., Ex.1007, 4:30-5:9.

196. In my opinion, a POSITA would have had a reasonable expectation of success in modifying *Kew*'s authentication system, which uses a conventional paging network to use a conventional cellular network, such as GSM, as taught by *Sormunen*, as such a task of making use of a different network and/or expanding

availability of an authentication system to more device types (including cell phones) was entirely routine for a POSITA. In sum, a POSITA would have been motivated to modify, and would have had a reasonable expectation of success in modifying, *Kew*'s authentication system to include *Sormunen*'s teachings related to the use of a cellular network.

**X. MY OPINIONS AS TO CLAIM 2 IN CONSIDERATION OF *KEW* IN VIEW OF *SORMUNEN* AND *KAUFMAN***

197. Claim 2 depends from claim 1, which I believe is rendered obvious by *Kew* in view of *Sormunen*.

**A. Claim 1**

198. As shown in the chart below, and with the exception of limitation 1[b], I understand claim 1 recites limitations analogous in scope to those of claim 5. For the corresponding sections referenced in the chart below, my opinions expressed in the corresponding section for limitations of claim 5 apply equally to the analogous limitations that appear in claim 1. For brevity, I am not going to repeat those opinions here again, but they of course apply equally here.

| <b>Claim 1 Limitation</b> | <b>Corresponding Analogous Claim 5 Limitation(s)</b> | <b>Section(s) that Apply Equally Here</b> |
|---------------------------|------------------------------------------------------|-------------------------------------------|
| 1[pre]                    | 5[pre], 5[e], 5[f]                                   | IX.A.1, IX.A.6, IX.A.7                    |
| 1[a]                      | 5[b], 5[e]                                           | IX.A.3, IX.A.6                            |
| 1[b]                      | <i>See Claim 7 and below</i>                         | IX.D                                      |
| 1[c]                      | 5[c]                                                 | IX.A.4                                    |
| 1[d]                      | 5[c]                                                 | IX.A.4                                    |

| <b>Claim 1 Limitation</b> | <b>Corresponding Analogous Claim 5 Limitation(s)</b> | <b>Section(s) that Apply Equally Here</b> |
|---------------------------|------------------------------------------------------|-------------------------------------------|
| 1[e] <sup>8</sup>         | 5[f]                                                 | IX.A.7                                    |
| 1[f]                      | 5[d]                                                 | IX.A.5                                    |
| 1[g]                      | 5[e]                                                 | IX.A.6                                    |
| 1[h]                      | 5[f]                                                 | IX.A.7                                    |

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

199. In my opinion, *Kew* in combination with *Sormunen* renders obvious this limitation. *See supra* Section IX.D (claim 7). As I also discussed with respect to Ground 2’s discussion of limitation 1[b] (Section VII.A, incorporated here), *Sormunen* discloses the elements of claim 1[b]. In the combination with *Kew* described with respect to claim 5, a POSITA would have understood that *Sormunen*’s “short message 2 [that] includes a **password request**” (Ex.1007, 5:35-6:1, Fig. 2) would be a request for a token (e.g., random code (Code A)).

200. Next, I note that the “paging service center 4 processes the incoming message and forms according to it a data transmission connection to a password server 5 and transmits the inquiry to it,” which “processes the message and forms a reply message containing one or more passwords and the user name in case a new

---

<sup>8</sup> In my opinion, this limitation is rendered obvious as discussed with respect to the section titled “Unified IPR Board Construction” in Section IX.A.7.

user is registered.” Ex.1007, 6:20-24. *Sormunen* describes that “[t]he present invention can be applied especially in such telecommunication systems in which it is possible to transmit short messages...on the basis of a terminal key, such as a telephone number” and that “[t]his quality is included in mobile communication systems,” which “include for example a **cellular system, a paging system, and a mobile phone system.**” Ex.1007, 4:30-5:8.

201. In my opinion, *Kew* in combination with *Sormunen* discloses *wherein the request* (e.g., a password request) *is transmitted by the user through the personal communication device* (e.g., receiver unit/paging terminal) *over the second network* (e.g., cellular network). As noted previously above, I provided further analysis concerning claim 7 (which recites aspects similar to 1[b]), and the analysis as to claim 7 applies equally to my opinions as to 1[b].

## **B. Claim 2**

202. Claim 2 adds “wherein the new password is generated by concatenating the token and the passcode.” In my opinion, *Kew* in combination with *Sormunen* and *Kaufman* renders obvious this limitation.

203. As I discussed previously, *Kaufman* discloses a system utilizing a password and a token, and that “workstation 516 **computes a ‘transmission code’ based upon the password and the token**” and that the transmission code is calculated by using a first ‘hashing algorithm.’” Ex.1008, 9:40-43. *Kaufman*’s

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

204. I note that *Kaufman* discloses different hashing algorithms that may be used to concatenate tokens and passcodes:

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

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

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

*Id.*, 9:65-10:5. As I discussed above, as the table above shows, *Kaufman* thus teaches concatenating the password onto the token, hashing the concatenation, and then again hashing the resulting hash value (1.1), concatenating the token onto the password and then hashing the concatenation (1.2), and also concatenating the password onto the token and then hashing the concatenation. Notably, the claim does not specify in which order the concatenation must occur (whether the token is concatenated onto the password, or vice versa) and, in any event, *Kaufman* discloses concatenating in any order. The claim also does not preclude the use of a hashing algorithm after concatenating the values, so *Kaufman* is directly on point in terms of teaching what claim 2 recites. I believe a POSITA would have appreciated that *Kaufman* discloses the generation of a password (*Kaufman*’s “transmission code”) through concatenation of a token and password. A POSITA would also have appreciated that *Kaufman*’s system is similar to the one claimed in the ’658 Patent. *See* Ex.1001, 4:52-53, Figs. 2A-2D. Indeed, the ’658 Patent

teaches “the user 108 can combine a valid memorized passcode of “abcd” with a valid token of “1234” to form a valid password of “abcd1234.” Ex.1001, 4:52-53; Figs. 2A-2D.

205. In my opinion, *Kew* in combination with *Sormunen* and *Kaufman* discloses *wherein the new password (e.g., transmission code) is generated by concatenating (e.g., the concatenating operation that occurs prior to application of Kaufman’s hashing algorithm) the token and the passcode.*

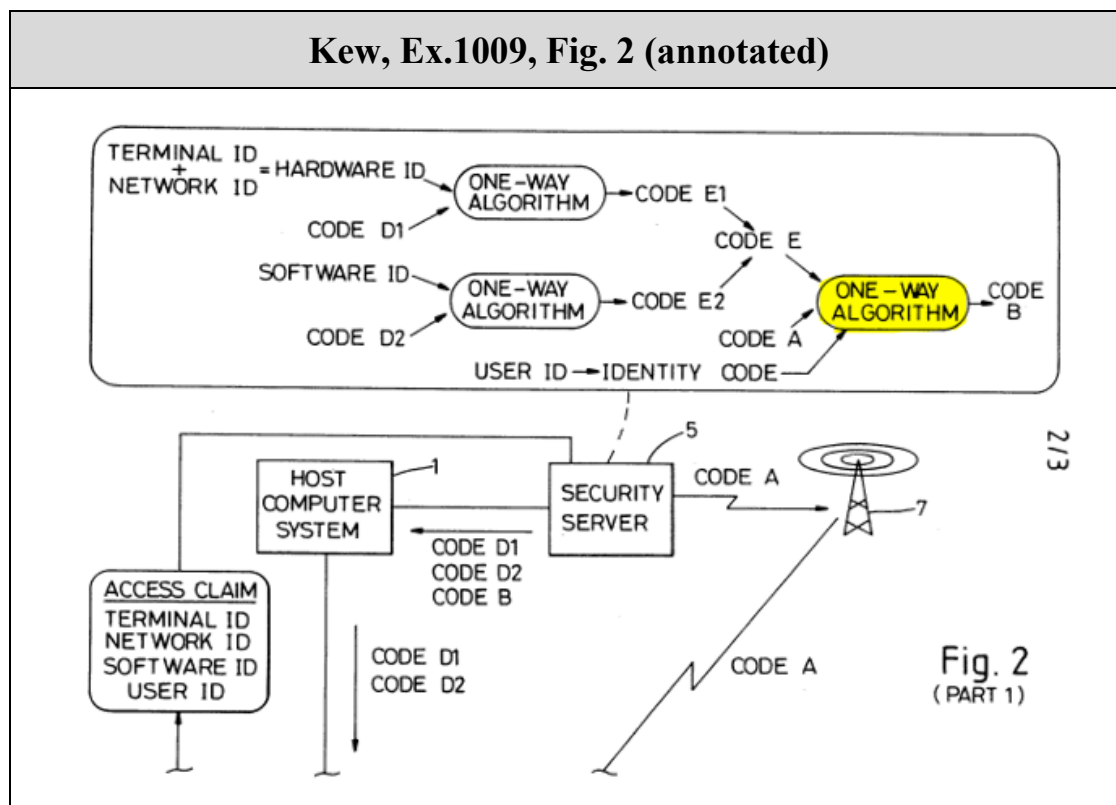
**C. A POSITA Would Have Been Motivated to Combine *Kew*, *Sormunen*, and *Kaufman***

206. In my opinion, a POSITA would have had ample motivation to implement the teachings of *Kaufman* with *Kew* and *Sormunen*.

207. ***First***, as I previously discussed in Section IX.C, a POSITA would have appreciated that *Kaufman* is within the same field of endeavor and is reasonably pertinent to a problem addressed in the ’658 Patent. *See* Section IX.C.

208. ***Second***, I believe a POSITA would have been motivated to combine the teachings of *Kaufman* with *Kew* and *Sormunen*’s teachings because the combination would have been an obvious result applying a known technique in another system to obtain improved and predictable improvements in security. *Kew* discloses that its system can be utilized in connection with encryption techniques and repeatedly discusses that its system utilizes transformation and one-way

algorithms to generate various codes. *See, e.g.*, Ex.1009, 7:34-8:10 (random Code A “encrypt[ed] using the same **one-way algorithm**...together with the corresponding identity code. In this way a transformed code (Code B) is produced.”), 7:20-32 (describing use of “**one-way algorithm**”); *see also id.*, 11:20-12:5 (“It then generates a second random number (Code D1) which is encrypted using a predetermined **one-way algorithm**, to produce a first transformed code (Code E1”), 12:19-34 (“The security key is now able to encrypt the received Code A using the Code F and the user identification code it contains via the **one-way algorithm** in its logic circuitry to produce the transformed code, Code C”), Fig. 2.



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

210. I believe a POSITA reviewing *Kew* and looking to implement its system would be motivated to look to another reference, such as *Kaufman*, that provides further details about exemplary one-way algorithms. Ex.1008, 9:41-10:17; *id.* (describing a “hashing algorithm” as “a **one-way routine**...[that] concatenate[es] selected items of the input data and perform[s] a ‘hashing equation’ upon one or more items of the input data, in a specified order.”).

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

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

212. **Third**, I note that because *Kew*’s system calls for a one-way algorithm for improving security and *Kaufman* discloses such a one-way algorithm through

the use of, for example, concatenation and hashing to achieve security and deter hacking, a POSITA would have had a reasonable expectation of success in modifying *Kew* in view of *Sormunen* and *Kaufman*. Indeed, in *Kew*, the invention notes that it provides for “an improved computer security system based on pager technology” as many large computer systems are subject to “hacking” attempts. Ex.1009, 1:7-18. A POSITA seeking to deter “hacking” attempts would have found *Kaufman*, as the reference discloses “an improved method by which a user or other principal in a computing system may authenticate to a computer system and establish a shared secret key for the protection of subsequent messages, with **reduced risk that the information in question will be improperly obtained or modified by a would-be intruder or imposter.**” Ex.1008, 1:13-19. By implementing the “cryptographically secure hashing algorithm” disclosed in *Kaufman* with the teachings of *Kew* and *Sormunen*, a POSITA would recognize that the security of information transmitted to the server would be improved. Ex.1008, 7:2-5.

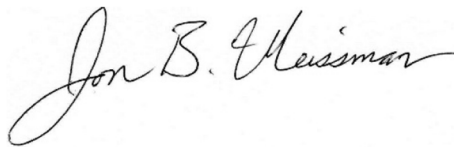
213. In my opinion, a POSITA would have been motivated to modify, and would have had a reasonable expectation of success in modifying, *Kew*’s authentication system to include *Sormunen*’s teachings related to the use of a cellular network and *Kaufman*’s teachings related to the use of a hashing algorithm.

## **XI. CONCLUSION**

214. For the reasons set forth above, in my opinion, all limitations of claims 2 and 7 of the '658 Patent are disclosed by the combinations of prior art cited herein.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the results of these proceedings.

Executed on December 18, 2023 in St. Paul, Minnesota

A handwritten signature in black ink, reading "Jon B. Weissman". The signature is written in a cursive, flowing style. Below the signature is a horizontal line.

Jon B. Weissman, Ph.D.

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

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

| <b>Claim No.</b> | <b>Claim Limitations</b>                                                                                                                                                                                                                                                                                                                                     |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | communication device configured to communicate over a cell phone network with the user authentication system;                                                                                                                                                                                                                                                |
| 5[c]             | a control module executed on the computer processor configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a password associated with the user to be the new password;                       |
| 5[d]             | a communication module configured to transmit the token to the personal communication device through the cell phone network; and                                                                                                                                                                                                                             |
| 5[e]             | an authentication module configured to receive the password from the user through a secure computer network, said secure computer network being different from the cell phone network,                                                                                                                                                                       |
| 5[f]             | wherein the user has an account on the secure computer network, wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account, such that said account is not accessible through any password via the secure computer network. |
| 6                | The system of claim 5, wherein the communication module is further configured to receive a request from the user for the token, and wherein the control module is further configured to create the new password in response to the request.                                                                                                                  |
| 7                | The system of claim 6, wherein the request is transmitted by the user through the personal communication device.                                                                                                                                                                                                                                             |