

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Experian Information Solutions, Inc.,

Petitioner

v.

Dynapass IP Holdings LLC,

Patent Owner.

IPR2023-01406

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

PETITION FOR *INTER PARTES* REVIEW UNDER 37 C.F.R. § 42.101

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. GROUNDS FOR STANDING.....	1
III. REASONS FOR THE REQUESTED RELIEF	1
IV. BACKGROUND	1
A. The '658 Patent	1
B. Prosecution History	6
C. Claim Construction	11
1. “Passcode,” “Token,” and “Password”	11
2. Order of Steps	12
D. Priority Date of the Challenged Claims	14
E. Person of Ordinary Skill in the Art	14
V. GROUNDS FOR CHALLENGE	15
VI. CLAIMS 1–7 ARE UNPATENTABLE UNDER 35 U.S.C. § 103.....	15
A. Sormunen, Perlman, and Motivation to Combine.....	15
1. Sormunen	15
2. Perlman	20
3. Motivation to Combine Sormunen and Perlman	22
B. Claims 1–7 are Obvious over Sormunen in view of Perlman.....	28
1. Claim 1	28

- a. 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: 28
- b. 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; 29
- c. receiving a request from the user for a token via the personal communication device, over the second network; 32
- d. 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; 34
- e. setting a password associated with the user to be the new password; 37
- f. activating access the user account on the first secure computer network; 38
- g. transmitting the token to the personal communication device; 38
- h. receiving the password from the user via the first secure computer network; and 39
- i. 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. 40

2.	Claim 2: The method of claim 1, wherein the new password is generated by concatenating the token and the passcode.	41
3.	Claim 3: The method of claim 1, wherein the personal communication device is a mobile phone.....	42
4.	Claim 4: The method of claim 1, wherein the personal communication device is a pager.....	43
5.	Claim 5	44
a.	A user authentication system comprising:.....	44
b.	a computer processor;	45
c.	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;	46
d.	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;	46
e.	a communication module configured to transmit the token to the personal communication device through the cell phone network; and	46
f.	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, 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.	47
6. Claim 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.....	47
7. Claim 7: The system of claim 6, wherein the request is transmitted by the user through the personal communication device.	47
VII. INSTITUTION DISCRETION	48
A. <i>General Plastic</i> Factors Favor Petitioner.....	48
B. <i>Fintiv</i> Factors Favor Petitioner.....	50
1. whether a stay has been granted or may be granted if a proceeding is instituted	51
2. proximity of the court’s trial date to the Board’s projected statutory deadline for a final written decision	51
3. investment in the parallel proceeding by the court and the parties	51
4. overlap between issues raised in the petition and in the parallel proceeding.....	52
5. whether the petitioner and the defendant in the parallel proceeding are the same party.....	52

6.	other circumstances that impact the Board’s exercise of discretion, including the merits.....	53
VIII.	MANDATORY NOTICES	53
A.	37 C.F.R. § 42.8(b)(1): Real Parties-in-Interest.....	53
B.	37 C.F.R. § 42.8(b)(2): Related Matters	53
C.	Lead and Back-Up Counsel and Service Information	55
IX.	PAYMENT OF FEES PURSUANT TO 37 C.F.R. § 42.103	55
	CERTIFICATE OF COMPLIANCE.....	57
	CERTIFICATE OF SERVICE	58

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Allied Erecting & Dismantling Co. v. Genesis Attachments, LLC</i> , 825 F.3d 1373 (Fed. Cir. 2016)	25
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020)	50
<i>Axionics, Inc. v. Medtronic, Inc.</i> , 73 F.4th 950 (Fed. Cir. 2023)	25
<i>Bank of America, NA v. Dynapass IP Holdings LLC</i> , IPR2023-00367, Paper 9 (P.T.A.B. July 18, 2023)	49
<i>General Plastic Indus. v. Canon Kabushiki Kaisha</i> , IPR2016-01357, Paper 19 (P.T.A.B. Sept. 6, 2017)	48, 50
<i>JPMorgan Chase & Co. v. Dynapass IP Holdings LLC</i> , IPR2023-01331, Paper 1 (P.T.A.B. Aug. 16, 2023)	48
<i>In re Keller</i> , 642 F.2d 413, 425 (CCPA 1981)	25
<i>Sotera Wireless, Inc. v. Masimo Corp.</i> , IPR2020-01019, Paper 12 (P.T.A.B. Dec. 1, 2020)	50
<i>Unified Patents, LLC v. Dynapass IP Holdings LLC</i> , IPR2023-00425, Paper 9 (P.T.A.B. July 18, 2023)	48, 49
Statutes	
35 U.S.C. § 102(a)	15
35 U.S.C. § 102(a) (2002)	20
35 U.S.C. § 102(b)	15
35 U.S.C. § 102(e) (2002)	20

35 U.S.C. § 311	1
35 U.S.C. § 314(a)	50, 53
35 U.S.C. § 325(d)	48

Other Authorities

USPTO Director Vidal, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (Memorandum, June 21, 2022) at 3, <i>available at</i> https://tinyurl.com/a6x9xnvj	50
--	----

EXHIBIT LIST

Exhibit No.	Description ¹
1001	U.S. Patent No. 6,993,658
1002	Certified File History for U.S. Patent No. 6,993,658
1003	Declaration of Stephen Perkins, Ph.D.
1004	PCT Publication No. WO 97/31306 (“Sormunen”)
1005	U.S. Patent No. 6,173,400 (“Perlman”)
1006	U.S. Patent No. 6,731,731 (“Ueshima”)
1007	U.S. Patent No. 5,881,226 (“Veneklase”)
1008	Japanese Patent Publication No. P2000-10927 (“Katou”)
1009	European Patent Publication No. EP1107089 (“Williamson”)
1010	U.S. Patent No. 5,787,169 (“Eldridge”)
1011	Hopcroft & Ullman, Introduction to Automata Theory, Languages, and Computation (1979) (ISBN: 0-201-02988-X)
1012	Carlo Ghezzi & Mehdi Jazayeri, Programming Language Concepts (1982) (ISBN 0-471-82173-X)
1013	Robert Sedgewick, Algorithms (1983) (ISBN 0-201-06672-6)
1014	Brian Kernighan & Dennis Ritchie, The C Programming Language (2d ed. 1988) (ISBN 0-13-110370-9))
1015	U.S. Patent No. 6,496,477 (Stephen J. Perkins, et al.)

¹ Descriptions are for convenience only and are not admissions or evidence.

Exhibit No.	Description ¹
1016	M. Wahl, “A Summary of the X.500(96) User Schema for use with LDAPv3,” RFC2256, Dec. 1997
1017	June 14, 2023, Docket Control Order, <i>Dynapass IP Holdings LLC v. Amazon.com, Inc.</i> , No. 2:23-cv-00063 (Lead Case) (E.D. Tex.) (ECF No. 57)
1018	April 21, 2023, Defendant Experian Information Solutions, Inc.’s Corporate Disclosure Statement, <i>Dynapass IP Holdings LLC v. Amazon.com, Inc.</i> , No. 2:23-cv-00063 (Lead Case) (E.D. Tex.) (ECF No. 20)
1019	July 7, 2023, Dynapass IP Holdings LLC’s First Supplemental Disclosure of Asserted Claims and Infringement Contentions
1020	April 17, 2023, Consolidation Order, <i>Dynapass IP Holdings LLC v. Experian Information Services, Inc.</i> , No. 2:23-cv-00066 (E.D. Tex.) (ECF No. 7)
1021	September 27, 2023, Defendant’s Stipulation Regarding Invalidity Contentions, <i>Dynapass IP Holdings LLC v. Amazon.com, Inc.</i> , No. 2:23-cv-00063 (Lead Case) (E.D. Tex.) (ECF No. 90)

I. INTRODUCTION

Experian Information Solutions, Inc. (“Experian” or “Petitioner”) hereby petitions for an *inter partes* review of claims 1–7 (“the Challenged Claims”) of U.S. Patent No. 6,993,658 (“the ’658 Patent”) (Ex-1001). Petitioner respectfully submits that the Challenged Claims are unpatentable under 35 U.S.C. § 103 and requests their cancellation. *See* 35 U.S.C. § 311.

II. GROUNDS FOR STANDING

Petitioner certifies under 37 C.F.R. § 42.104(a) that the ’658 Patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting an *inter partes* review of the Challenged Claims on the grounds identified herein. This Petition is complete pursuant to 37 C.F.R. § 42.106(a).

III. REASONS FOR THE REQUESTED RELIEF

As explained below and in the attached Declaration of Petitioner’s expert, Dr. Stephen Perkins (Ex-1003), the authentication method and system of the Challenged Claims was obvious over the prior art to a person of ordinary skill in the art (“POSA”) at the time of the claimed invention.

IV. BACKGROUND

A. The ’658 Patent

The ’658 Patent is titled “Use of Personal Communication Devices for User Authentication,” and was filed on March 6, 2000. The ’658 Patent relates

“generally to the authentication of users 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. The ’658 Patent has seven claims: method claims 1–4 and system claims 5–7.

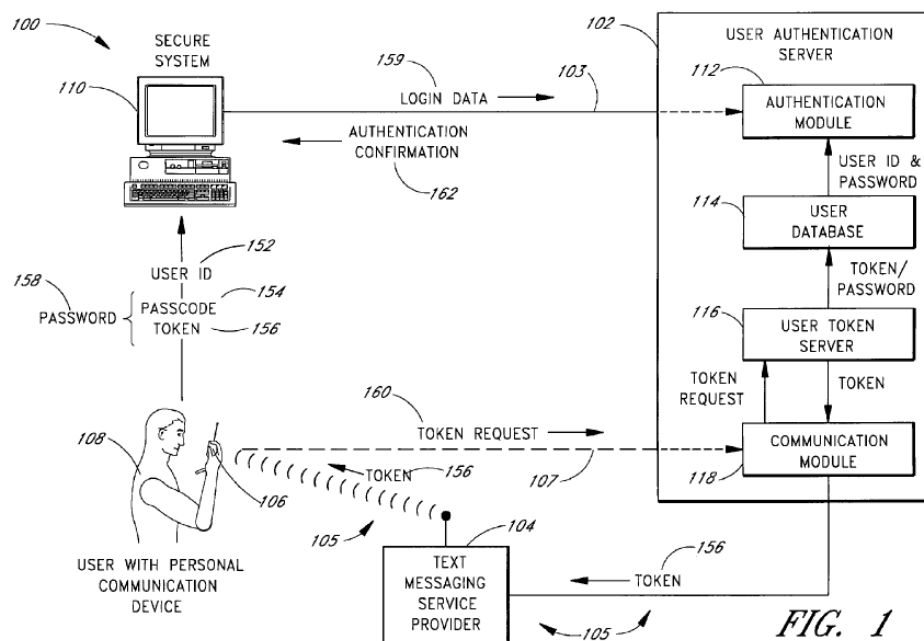
The ’658 Patent notes that systems “typically require the submission of a user ID and password combination” for access. *Id.*, 1:15–20. The ’658 Patent provides that “[p]asswords created by users are often combinations of words and names, which are easy to remember but also easily guessed” by “hackers.” *Id.*, 1:28–31. As a consequence, “many systems impose regulations on password formats,” but this can make passwords hard to remember and can “result[] in the password being written down,” creating a security risk. *Id.*, 1:31–43.

The ’658 Patent indicates that “requiring a two-factor authentication process” was a known solution. *Id.*, 1:44–46. The ’658 Patent notes that RSA Security Inc. was distributing the “SecurID product” for two-factor authentication. *Id.*, 1:44–46. The first factor is something the user knows (“a user passcode or personal identification number”) and the second factor is a something “possessed by the user”—“a SecurID card.” *Id.*, 1:46–48. The ’658 Patent provides that “[t]he SecurID card generates and displays unpredictable, one-time-only codes that automatically change every 60 seconds. The user supplies the displayed code upon

logging into a system.” *Id.*, 1:49–52. The system verifies it with “a corresponding code generator.” *Id.*, 1:52–53.

The ’658 Patent notes that instead of carrying an “additional item,” it would be more convenient “[i]t would be advantageous if the benefits of the SecurID system could be achieved using a device that many users already carry—a personal communication device such as mobile phones or pagers.” *Id.*, 1:55–60.

The ’658 Patent discloses “a password setting system for setting user passwords for a secure system, such as a computer system or a secure area of a building.” *Id.*, 1:63–66. FIG. 1 of the ’658 Patent depicts “user authentication system 100 according to a preferred embodiment of the present invention.” *Id.*, 4:2–4.



Ex-1001, FIG. 1.

The '658 Patent provides that “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.

Instead of getting the second factor from a code generator, the '658 Patent discloses requesting one through a phone call or text, or through a user interface. *See, e.g., id.*, 4:63–65, FIGs. 2C-D, 6:26–32. The '658 Patent refers to this requested information as the “token.” The requesting personal communication device is identified as a user’s device because of an association of the user ID with the phone number, which can be stored in “any database capable of storing user ID and password data.” *Id.*, 2:33–35, 5:20–21. The '658 Patent discloses that a “token” is generated by “any number of methods that preferably produces a random or pseudorandom sequence of numbers and/or digits.” *Id.*, 6:53–55. This “token” is then sent to the personal communication device, and may be time-limited. *Id.*, 4:42–45, 9:61–54.

The disclosed password-setting system of the '658 Patent generates a password based on the passcode and token. *Id.*, FIG. 3. The '658 Patent discloses that the new password is “preferably create[d]” by “combining the user’s passcode 154, which is stored by the user token server 116, with the newly generated token 156.” *Id.*, 6:59–63. The '658 Patent further discloses that the password is

“preferably generated by concatenating the passcode 154 and the token 156.” *Id.*, 9:31–32. The only example given by the ’658 Patent is a passcode of “abcd” and a token of “1234,” and the password being “abcd1234.” *Id.*, 4:52–56. The ’658 Patent discloses that in the preferred embodiment, the user enters the password in a login screen, as shown in FIG. 2A. *Id.*, 4:52–63. Alternatively, the user enters the passcode and token separately, as shown in FIG. 2B. *Id.*

The user is able to access the secure system by “logging in using the supplied token 156.” *Id.*, 9:55–60. The user uses it for logging in by submitting it with the user’s passcode (*see, e.g.*, FIG. 2B), or by concatenating the passcode and token to form a “password” (*see, e.g.*, FIG. 2A). *See, e.g., id.*, 5:8–10 (“authenticating a user based upon a supplied user ID 152 supplemented by a supplied password 158 or a passcode 154 and a token 156 combination”), 7:42–45, 9:54–60 (“The user 108 preferably concatenates his memorized secret passcode 154 with the valid token 156 to create the password 158.”).

Logon To Network:

USER ID

PASSWORD

Note: Your password is your passcode followed by a valid token

FIG. 2A

Logon To Network:

USER ID

PASSCODE

TOKEN

FIG. 2B

B. Prosecution History

The application from which the '658 Patent issued, U.S. Patent Application No. 09/519,829 (“the '829 application”), was filed on March 6, 2000.

All original 27 claims were cancelled and 26 new claims (28–53) presented in a preliminary amendment, starting with claim 28, shown below.

28. A method of authenticating a user, the method comprising:
 associating the user with a personal communication device possessed by the user;
 generating 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;
 setting a password associated with the user to be the new password;
 transmitting the token to the personal communication device; and
 receiving the password from the user.

Ex-1002, 157.

The claims were rejected on December 15, 2003. Ex-1002, 181–187. Claims 37–39 were rejected as anticipated by Australian Patent Application No. 63545/98 by Schmitz. *Id.*, 184. Claims 28–36 and 40–53 were rejected as obvious over Schmitz in view of the Handbook of Applied Cryptography by Menezes. *Id.*, 185–86. The examiner identified that “it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the system disclosed by Schmitz by creating a password using the user’s password information in addition to an ID for the device (the token), using a hashing function, as disclosed by Menezes, in order to make dictionary attacks less effective.” *Id.*, 186.

In response, the applicants argued that Schmitz makes and receives a request from the same device and that Schmitz does not teach associating a user with a personal communication device possessed by the user. *Id.*, 234–239.

Claims 28–31 and 43–53 were subsequently rejected again on May 24, 2004, as anticipated by U.S. Patent No. 5,323,146 to Glaschick. *Id.*, 245. Claims 37–39 were rejected as anticipated by U.S. Patent No. 6,226,364 to O’Neil. *Id.*, 245–246. Claims 32–36 and 40–42 were rejected as obvious over O’Neil and Glaschick. *See id.*, 242–248.

In response, the applicants argued that Glaschick failed to “associating the user with a personal communication device possessed by the user,” “wherein the request is transmitted from a personal communication device,” and “transmitting the token to the personal communication device.” Ex-1002, 258–260. The applicants also argued that there was no teaching, suggestion, or motivation to combine Glaschick with O’Neil. *Id.*, 262–263.

All claims were rejected again on February 7, 2005, in a final rejection that maintained the rejections based on Glaschick and O’Neil. *Id.*, 266–274. The examiner found: “[T]he data station as disclosed by Glaschick may be a computer with programs (see column 1, line 15), and clearly has communication capability. Applicant’s personal communication device, as viewed in light of Applicant’s specification, is simply a type of computer with programs; therefore, the claimed

invention is anticipated.” Ex-1002, 271. Regarding combining Glaschick with O’Neil for obviousness, the examiner further found that “one skilled in the art would recognize that the motivation supplied by Glaschick would apply to any computerized system having authentication.” *Id.*, 272–273.

Following an examiner’s interview (*id.*, 276–277), the applicants amended the claims to overcome the final rejection (*id.*, 280–285). The amendments to independent claim 28 (issued claim 1) are reproduced below.

Listing of Claims

Claims 1-27 (Canceled)

Claim 28 (Currently amended): 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:

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;

receiving a request from the user for a token via the personal communication device, over the second network;

generating a new password for said first secure computer network based at least upon [[a]] the token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user;

setting a password associated with the user to be the new password;

activating access the user account on the first secure computer network;

transmitting the token to the personal communication device; [[and]]

receiving the password from the user via the first secure computer network; and

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.

Ex-1002, 281.

Following the amendments to the claims (including cancellation of claims 30–31 and 37–53), a notice of allowance was issued on August 8, 2005. Ex-1002, 289–296. The examiner’s “statement of reasons for allowance” was that “no art could be found wherein the transaction for determining the password in setting up of a new calling-card-derived temporary network account is performed entirely over a connection other than that used by [the] eventual network account.” *Id.*, 294–295. The examiner also found: “Some of the closest art, the ‘Monkey Technical Overview’ (see IDS filed 23 May 2000), sets up a password for a temporary account, but the user request is sent over the network account connection.” *Id.*, 295.

The Monkey Technical Overview, dated July 15, 1999, discloses:

The mobile network key (“monkey”) one-time password system for secure two-factor ‘what you have and what you know’ user authentication. In contrast to other hardware-based solutions, which depend on their own proprietary infrastructure to be established – by handing a hardware authentication token to each user -, monkey employs an existing world-wide infrastructure, the global GSM network for digital telephony, and thus turns any GSM mobile telephone into an authentication token.

Ex-1002, 94. The reference discloses transmitting requested passwords to users over a cell phone network that is separate from the “network account connection”:

monkey makes use of this GSM service to efficiently transmit one-time passwords via a separate channel, i.e. the GSM network, to users requesting authentication. Suppose Alice would like to authenticate herself. To do so, she initiates a connection to the point of authentication, e.g. a telnet session to a firewall machine. After having identified herself by means of a user name and, at the discretion of her security administrator, a fixed password, a temporary one-time password, transmitted by monkey, appears on the display of her mobile phone. Alice reads the password off the display, types it in and, in case she performed well, is granted access.

Id.; Ex-1003, ¶¶ 71–73. As indicated by the examiner, the Monkey Technical Overview discloses:

- A secure computer network on which the user has an account: the user “initiates a connection to the point of authentication, e.g. a telnet session to a firewall machine” where the user identifies herself with a “user name.”
- A database of users and their mobile phone numbers.
- A passcode known to the user: “a fixed password.”
- A token not known to the user (at least prior to it being generated and sent to her in response to her request): “a temporary one-time password” that is sent to the user’s mobile phone and she reads “off

the display, types it in and,” if entered correctly, “the user is granted access.”

Ex-1002, 94–99; Ex-1003, ¶ 73. Thus, according to the examiner, the missing teaching in the prior art was the user’s request being sent over the separate cell phone network rather than “over the network account connection.” Ex-1002, 295; Ex-1003, ¶ 73.

C. Claim Construction

Petitioner proposes that each claim term be given its plain and ordinary meaning as would be understood in the context of the specification and prosecution history, and that no specific construction of any claim term is required in this proceeding because the ground identified in this Petition demonstrates the unpatentability of the claims under any reasonable construction. Petitioner addresses the terms “passcode,” “token,” and “password,” as well as the ordering of steps with respect to the creation of the password and the transmission of the token to the user’s personal communication device.

1. “Passcode,” “Token,” and “Password”

A POSA would understand that “passcode,” “token,” and “password” refer to strings with different labels according to their function or role. Ex-1003, ¶ 125; *see also* Ex-1003, ¶¶ 89–102. The example in the ’658 Patent is a “memorized passcode of ‘abcd,’ a valid token of ‘1234,’” and forming the password

“abcd1234.” Ex-1001, 4:52–56. The ’658 Patent provides that a “passcode” is a “secret [string] known to the user.” *Id.*, 2:13–14 (“secret information known to the user, such as the passcode”); Ex-1003, ¶ 125; *see also* Ex-1003, ¶¶ 88–101. It is information that can be associated with a user ID. Ex-1001, 8:53–55 (“[T]he control module 402 associates a user ID with a passcode 154 and phone number of a user’s personal communication device 106.”). A token is a string “that is provided to the user through an object possessed by the user.” *Id.*, 2:14–15; Ex-1003, ¶ 125; *see also* Ex-1003, ¶¶ 89–102. The password is a string generated based on the token and the passcode, such as by combining or concatenating them. Ex-1001, 2:2–4 (“The server creates a new password by concatenating a secret passcode that is known to the user with the token.”); Ex-1003, ¶ 124; *see also* Ex-1003, ¶¶ 89–102.

2. Order of Steps

Claim 1 recites: “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.” Claim 1 also recites: “transmitting the token to the personal communication device.”

Similarly, claim 5 recites: “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.” Claim 5 also recites: “a communication module configured to transmit the token to the personal communication device through the cell phone network.”

It could be assumed that the token becomes known to the user when it is transmitted to the personal communication device. Thus, the password would have to be created prior to transmission of the token to the personal communication device. Ex-1003, ¶ 123. FIGs. 2A and 2B, for example, show that the user is given the token so that he or she can type it into the user interface. Ex-1001, FIGs. 2A and 2B. The '658 Patent also provides: “In the preferred embodiment, the user 108 combines the passcode 154 and the token 156 by concatenation to form the password 158.” Ex-1001, 7:42–45; Ex-1001, 9:54–60 (“The user 108 preferably concatenates his memorized secret passcode 154 with the valid token 156 to create the password 158.”). The user could not do so if the token did not become known to the user. Ex-1003, ¶ 123.

However, it does not affect the unpatentability of the Challenged Claims on the ground asserted in this Petition. The prior art teaches the token being requested by and transmitted to a user over a cellular network via a personal communication device and then automatically provided by the personal communication device to a computer terminal through which the user authenticates to an account on a secure

computer network. Ex-1003, ¶¶ 124, 176. The prior art also teaches using a mobile device's display to show the token to the user. *Id.* Thus, the prior art teaches at a minimum for purposes claims 1 and 5 that the token is not known to the user at the time the password is created, and at a maximum does not become known to the user even when the password is submitted. Thus, while the prior art also teaches that the token may subsequently become known to the user, it does not alter the unpatentability of the claims. *Id.*

D. Priority Date of the Challenged Claims

The earliest priority date for the '658 Patent is the filing date: March 6, 2000.

E. Person of Ordinary Skill in the Art

A POSA with respect to the '658 Patent would have had a bachelor's degree in computer science, management of information systems, or electrical engineering, or similar field, with one-to-two years of experience in the design, support, or implementation of systems requiring user authentication. Additional education may substitute for experience with user authentication. Likewise, additional relevant experience with user authentication may substitute for education. Ex-1003, ¶ 48. Additional education may substitute for experience with user authentication, and additional experience with user authentication may substitute for education. *Id.*

V. GROUNDS FOR CHALLENGE

The Challenged Claims of the '658 Patent are unpatentable under 35 U.S.C.

§ 103 on the following ground:

Ground	Claims	Reference(s)
1	1–7	Sormunen in view of Perlman

VI. CLAIMS 1–7 ARE UNPATENTABLE UNDER 35 U.S.C. § 103

A. Sormunen, Perlman, and Motivation to Combine

1. Sormunen

Sormunen (Ex-1004) is an international patent application filed on February 6, 1997. Sormunen was published on August 28, 1997, and claims priority to a Finnish patent application filed on February 23, 1996. Sormunen is prior art under at least 35 U.S.C. § 102(a) and (b).

Sormunen discloses “a method and system for obtaining at least one item of user specific authentication data, such as a password and/or a user name.” Ex-1004, 1:3–5. A POSA would understand that a token could also be one item of user specific authentication data. Ex-1003, ¶ 128. Sormunen discusses the use of “information services,” which can be connected to via a “data transmission connection” over a “telecommunication network or a mobile communication network.” Ex-1004, 1:8–13. To use the information service, “user specific authentication data is required, for example a user name and password.” *Id.*, 1:14–

15. The user name and password “enable the information service provider to control the user using the information service” and “prevent unauthorized use of the information service.” *Id.*, 1:17–22.

Sormunen discloses that “[a] user name is user specific and it is usually not changed in different connection set-ups.” Ex-1004, 1:30–31. Regarding passwords, Sormunen discloses that the use of “[o]ne single password valid as long as the user is a registered subscriber to the service” is “used mainly used in services with less need for security.” *Id.*, 1:34–36. Sormunen discloses that an alternative is “[a] list of single-connection passwords, each valid for one connection.” *Id.*, 2:1–2. However, a drawback of this approach is “that the list has to be kept safe and account of the last used password has to be kept in one way or another. Thus the possibility of abuse is great, especially if the list and the user name are preserved in the same place.” Ex-1004, 2:20–24. Sormunen discloses that another option is “[a] periodical password valid for a predefined period of time.” *Id.*, 2:13. However, Sormunen further discloses that “regardless of which password type is used, it is the user of the service who is to a great extent responsible for data security, and the service provider has few possibilities to prevent and control abuse for example in case the password falls into the wrong hands.” *Id.*, 2:26–29.

Fig. 2 of Sormunen “shows a method for transmitting a user name and passwords according to a preferred embodiment of the invention.” Ex-1004, 5:26–27.

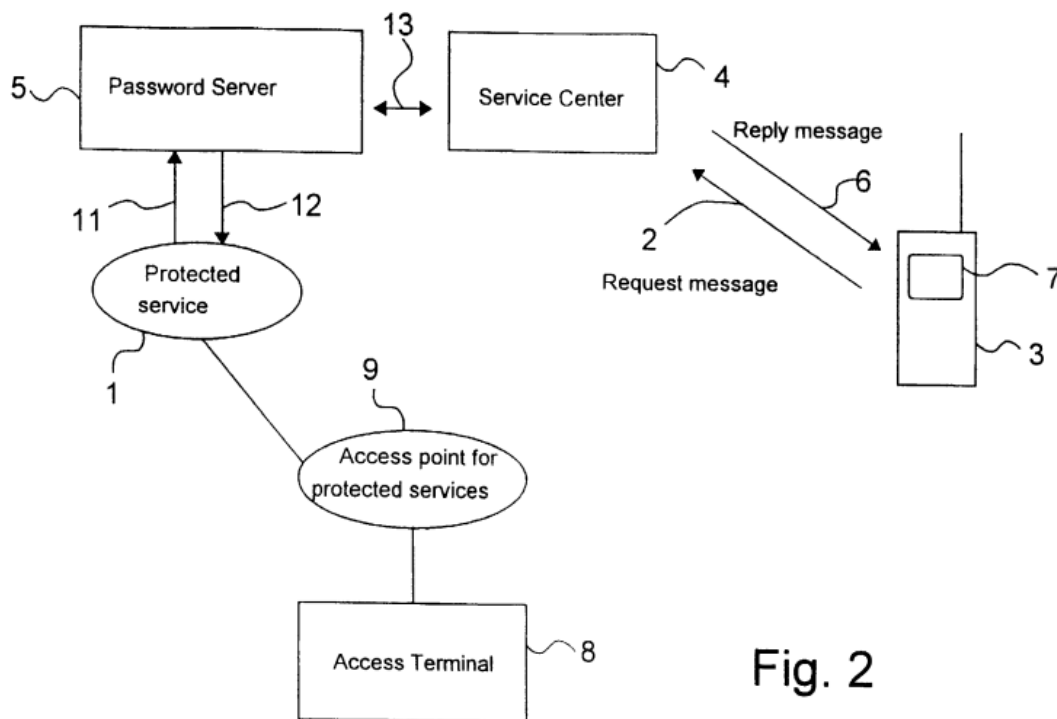


Fig. 2

Ex-1004, FIG. 2.

A user wishing to use “protected service 1” can obtain “a password” or “list of passwords” to use it. Ex-1004, 5:35–37. To do so, “the user of the service sends a short message 2 from the paging terminal 3, such as a mobile station.” *Id.*, 5:33–38.

Sormunen discloses that “[t]he short message 2 includes a password request and possibly also a subscription request for a new user.” *Id.*, 5:38–6:2. The user sends short message 2 to “paging service center 4,” which “is for example in the

GSM system advantageously a short message service center.” Ex-1004, 6:32–33; Ex-1004, 5:6–8 (“It is advantageous to apply the present system in mobile communication systems which include short message service (SMS) or paging.”). The “GSM system” is disclosed as “a mobile communication system in which a cellular network is used.” *Id.*, 6:1–3. Sormunen provides that “[t]he form of the data depends on the type of the message system used. For example the GSM system allows sending short messages, wherein a GSM mobile station can be used in implementation of the method according to the invention.” *Id.*, 6:4–7.

The paging service center 4 processes the request and “transmits the inquiry to” “password server 5.” Ex-1004, 6:20–23. “The password server 5 processes the message and forms a reply message containing one or more passwords and the user name in case a new user is registered.” *Id.*, 6:23–24. “The password server 5 transmits the password and/or user name to the short message service center 4, which forms according to the data a reply message 6, which is sent to the paging terminal 3 preferably in enciphered form.” *Id.*, 6:35–38. The reply can be shown to the user, such as by using display means 7 of paging terminal/mobile station 3. *Id.*, 7:4–6.

The user can use “Access Terminal” 8 to form a data transmission connection to the verification service 9 of protected service 1. *Id.*, 7:9–10. Access terminal 8 is also disclosed as data processor 8, and can communicate with the

protected service 1 (information service) through “a modem connection to a wireline telecommunication network.” Ex-1004, 8:5–7. The user submits a user name and password through access terminal 8 to verification service 9. *Id.*, 7:9–13.

“[T]he verification service 9 transmits the given data to the service 1, which sends a check request 11 of the user name and the password to the password server 5.” Ex-1004, 7:11–14. “The password server 5 examines the data and communicates in a reply message 12 to the service 1 whether the user name and the password are given correctly,” and if they are, the user is given a data transmission connection to the service 1. If they are not correct, the user is prevented from using the service. *Id.*, 7:14–18.

Sormunen further discloses: “[T]he present invention can be applied also for obtaining a personal identity number (PIN) of bank and credit cards and corresponding charge cards. Thus when the charge card is being ordered, the number of the orderer’s paging device or mobile station can be given, wherein the supplier of the charge card transmits the personal identity number connected to the charge card to the paging device or the mobile station of the user.” *Id.*, 9:26–32. “The method according to the invention can be used for requesting a new personal identity number for a charge card which is already in use, wherein the identity number is transmitted to the paging device or the mobile station of the user.” *Id.*, 9:34–37.

Sormunen is analogous art to the '658 Patent. Sormunen is from the same field of endeavor as the '658 Patent: user authentication. Ex-1003, ¶ 137. Further, Sormunen is reasonably pertinent to at least one problem relevant to the inventors of the '658 Patent. *Id.* For example, the inventors of the '658 Patent were concerned with eliminating the need for an additional device to provide user authentication information by instead providing it using “a device that many users already carry—a personal communication device such as mobile phones or pagers.” Ex-1001, 1:55–60. Sormunen discloses using a paging terminal/mobile station to communicate using short messages over a cellular network to request and receive user authentication information. Thus, Sormunen was reasonably pertinent to at least one problem relevant to the inventors the '658 Patent. Ex-1003, ¶ 137.

2. Perlman

U.S. Patent No. 6,173,400 to Radia J. Perlman, et al. (“Perlman”), has a filing date of July 31, 1998. Ex-1005. Perlman is prior art under at least pre-AIA 35 U.S.C. § 102(a) and pre-AIA 35 U.S.C. § 102(e).

Perlman relates to “secure communications, and more particularly, to methods and systems for establishing a shared secret between devices connected over a communication medium using an authentication token to provide user authentication, data encryption, and integrity protection.” Ex-1005, 1:6–11.

Perlman discloses that “a user name and password only provides a minimal level of use authentication to access the network” and that “[i]f the password is simple (e.g., the user’s birth date) a hacker can easily determine the user’s password and access the network with this information assuming the user’s name.” Ex-1005, 1:25–27.

In light of the aforementioned vulnerabilities, Perlman discloses “using an authentication token to provide adequate user authentication, data encryption, and integrity protection.” *Id.*, 3:10–12. Specifically, Perlman discloses using “an authentication token that generates a character string” that may be, for example, “a password based on the time of day encrypted with a secret code or a random number.” *Id.*, 4:44–48. The “character string is communicated to a local device (e.g., a work station) where it can be modified using a predetermined function to produce a result (i.e., a second character string).” *Id.*, 4:48–51. The resultant “second character string” is communicated to the remote device for authentication. *Id.*, 4:51–64.

Perlman is analogous art to the ’658 Patent. Perlman is from the same field of endeavor as the ’658 Patent: user authentication. Even if it was not, Perlman was reasonably pertinent to at least one problem relevant to the inventors of the ’658 Patent. Ex-1003, ¶ 145. For example, the inventors of the ’658 Patent specifically were concerned with two-factor authentication using “what you have”

and “what you know.” Ex-1001, 1:44–54, 2:1–11. Perlman is also concerned with two-factor authentication based on “what you have” and “what you know.” Ex-1005, 1:38–41. Further, the inventors of the ’658 Patent were concerned with passwords being secure and not being guessed by hackers. Ex-1001, 1:20–31. Perlman discusses the same concern and discusses approaches for forming more secure passwords from known and generated strings. Ex-1005, 1:24–28. The inventors of the ’658 Patent sought to obtain the benefits of using devices like the SecurID card, just using a mobile phone or pager instead. Ex-1001, 1:56–59. Thus, the ways of using codes generated by the token devices as disclosed by Perlman would still be relevant to the inventors of the ’658 Patent when seeking at least to address creating more secure passwords. Ex-1003, ¶ 145.

3. Motivation to Combine Sormunen and Perlman

A POSA would have found it obvious as of March 6, 2000, to combine the teachings of Sormunen with the teachings of Perlman. A POSA would have been motivated to modify Sormunen with the teachings of Perlman to allow for greater security and ease of use. Ex-1003, ¶ 146.

Sormunen concerns generating passwords for new subscribers to an information service. Sormunen discloses that in the prior art, a user wishing to gain access to an information service would send a request for a subscription, be sent a form, fill out the form, and send it back to the service provider. Ex-1004, 2:31–35,

3:12–18. “The information service provider subsequently handles the form and allots the user the user specific authentication data and sends it for instance by mail, electronic mail or facsimile (block 107).” *Id.*, 3:19–21. After receiving the user specific authentication data, the user can start using the information service. *Id.*, 3:21–22. The “user specific authentication data” is “for example a user name and password.” *Id.*, 1:14–15.

Sormunen “enables very fast subscription” including “transmission of user information in enciphered electronic form and the receiver can be recognized in order to prevent abuse.” Ex-1004, 5:10–18. Sormunen provides that “[a] further advantage of the fast data transmission is that the validity of passwords can be shortened remarkably and security may thus be improved.” *Id.*, 5:16–18.

Sormunen discloses “[t]he transmission of user specific authentication data to the user is performed by using paging or short message service.” Ex-1004, 9:22–24. Sormunen also discloses generating a new PIN and transmitting it to a user’s paging device or mobile station. *Id.*, 9:34–37. A POSA would appreciate that this could be a “single-connection” password or PIN, and/or a password or PIN “valid for a predefined period of time.” *Id.*, 2:1–18; Ex-1003, ¶ 149.

This would also allow greater flexibility in letting users select their own password when registering with the service provider. Ex-1004, 3:31–32; Ex-1003, ¶ 150. By requiring that this selected or initial password be augmented by a

generated PIN to create an account password (one that must be created in order for the account to be accessed) the level of security would be increased according to known methods. Ex-1003, ¶ 150.

Perlman discloses that “a user name and password only provides a minimal level of use authentication to access the network” and that “[i]f the password is simple (e.g., the user’s birth date) a hacker can easily determine the user’s password and access the network with this information assuming the user’s name.” Ex-1005, 1:25–27. Sormunen does not solve the recognized security issue concerning user name and password combinations. Thus, a POSA would have been expressly motivated to combine the teachings of Perlman with the teachings of Sormunen to increase security (i.e., minimize the ability of unauthorized third parties to determine a user’s password). Ex-1003, ¶¶ 151–152.

Sormunen notes that “the service provider has few possibilities to prevent and control abuse for example in case the password falls into the wrong hands.” Ex-1004, 2:26–29. A POSA would have recognized that combining the teachings of Sormunen with the teachings of Perlman would have provided a greater ability to prevent and control abuse. Even if the third party obtained the user’s initial or selected password, the third party would have to, at a minimum, also obtain the user’s new PIN. Ex-1003, ¶ 153.

Further, a POSA would have been motivated to combine the teachings of Perlman without incorporating the “authentication token” device disclosed in Perlman. Ex-1003, ¶ 153. “The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference[.]” *Allied Erecting & Dismantling Co. v. Genesis Attachments, LLC*, 825 F.3d 1373, 1381 (Fed. Cir. 2016) (quoting *In re Keller*, 642 F.2d 413, 425 (CCPA 1981)); *Axonics, Inc. v. Medtronic, Inc.*, 73 F.4th 950, 957 (Fed. Cir. 2023) (“[A] skilled artisan may be motivated to combine particular features of different references, e.g., to secure some benefits at the expense of others, even when bodily incorporation would be impossible or inadvisable.”). Sormunen discloses requesting and sending user authentication information via SMS to the paging terminals/mobile stations of users, including the disclosed capability of generating and sending new PINs in response to requests. Ex-1003, ¶ 153. A POSA would appreciate that user-selected passwords as disclosed by Sormunen would be vulnerable to attack. *Id.* Sormunen also expresses a need for ways to “to prevent and control abuse for example in case the password falls into the wrong hands.” Ex-1004, 2:26–29. Using a generated code with a known password for greater security was a well-known technique to address these issues. Ex-1003, ¶¶ 76–80. Perlman refers to a known “PIN” and generated code, but, as articulated above (Section IV.C.1), the difference in labeling does not affect how a POSA would

view them. *Id.*, ¶ 125. A string known to the user and the system is combined with a generated string to form a string needed for authentication. Ex-1003, ¶¶ 125, 153–154; *see also* Ex-1003, ¶¶ 89–102.

It was well-known to use a reusable password with a one-time password for two-factor authentication. Ex-1003, ¶¶ 76–80, 154. It was a predictable variation to combine a reusable password with a one-time password and use that for authentication. Ex-1003, ¶¶ 153–154.

Further, combining the teachings of Sormunen with the teachings of Perlman would have involved applying a known technique (concatenation of a generated string to a known string) to achieve predictable results (increased security). Ex-1003, ¶ 153. It was a known technique to concatenate a generated string with a known/preexisting string (password), and known that it would result in a stronger, more secure password. *Id.*

A POSA would have appreciated that the resulting character string could be used more securely as a password than the original known secret character string. *Id.* Thus, a POSA would have been motivated to combine the teachings of Perlman with Sormunen. *Id.* The original password set for the user (including one proposed by the user) could be augmented by concatenating it with a generated PIN. A POSA would appreciate that, according to the teachings of Perlman, this predetermined function (concatenation) would be known to the password server.

Id. Thus, the password server generates a PIN, and then sets the password as the concatenation of the preexisting or initial password and the PIN, which may be randomized according to techniques known to POSAs. *Id.* The PIN (user authentication information) would then be transmitted to the user via the user's paging terminal/mobile station. *Id.*

A POSA would have had a reasonable expectation of success in modifying Sormunen with the teachings of Perlman to achieve what is claimed in the '658 Patent and would have needed only routine skill to do so. Ex-1003, ¶ 155. Combining the teachings of Sormunen and Perlman was within the skill of a POSA. *Id.* The modification would have operated in a predictable manner consistent with the state of the art. *Id.* Further, Perlman discloses that “authentication techniques consistent with the present invention may be used on” the Internet as well as “other WANs as well as local area networks (LANs), network protocols, and other communication media.” Ex-1005, 5:34–45; Ex-1003, ¶ 155.

Perlman discloses that “a user name and password only provides a minimal level of use authentication to access the network” and that “[i]f the password is simple (e.g., the user's birth date) a hacker can easily determine the user's password and access the network with this information assuming the user's name.” Ex-1005, 1:25–27. Sormunen does not solve the recognized security issue

concerning user name and password combinations. Thus, a POSA would have been expressly motivated to combine the teachings of Perlman with the teachings of Sormunen to increase security (i.e., minimize the ability of unauthorized third parties to determine a user's password).

B. Claims 1–7 are Obvious over Sormunen in view of Perlman

1. Claim 1

- a. 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:**

If the preamble is limiting, Sormunen discloses a new or preexisting user wishing to gain access to protected service 1 (*first secure computer network*), which requires a user name particular to that user (*the user having a user account on said first secure computer network*). Ex-1004, Fig. 2, 5:33–6:2; Ex-1003, ¶ 158. As shown in and described with respect to Fig. 2, a user can use an access terminal/data processor to connect to the protected service (electronic information service) through “a modem connection to a wireline telecommunication network.” Ex-1004, 8:5–7; Ex-1003, ¶ 158. The “first secure computer network” is highlighted in orange in Fig. 2 below.

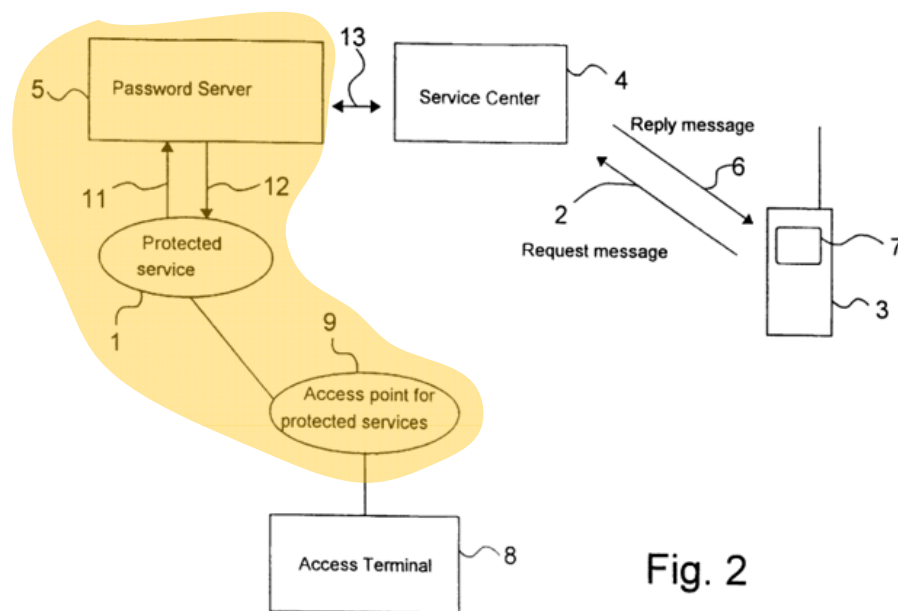


Fig. 2

Ex-1004, FIG. 2 (annotated).

- b. 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;

As discussed above, Sormunen discloses a user wishing to gain access to a protected service (*first secure computer network*). Ex-1004, Fig. 2, 5:33–6:2. Sormunen discloses the use of a “paging terminal” or “mobile station” by a user (*personal communication device*). Ex-1004, 5:35–6:7.

Sormunen discloses “[w]hen a new user starts using the information service, the user has to register to the information service provider. This may be done for example by a written subscription request, in which the user gives his or her

personal data and other information required, most often by mail, electronic mail (e-mail) or facsimile. In due course, the new user is sent a user name and a password or a list of passwords.” Ex-1004, 2:31–38. Sormunen further discloses that this can be done via forms displayed on the “data processor,” with “[i]nformation to be filled in include e.g. forename, surname, a proposal for user and password.” Ex-1004, 2:31–32. Sormunen discloses that the information service provider “forms a record or the like for the user, in which the data of the new user is saved.” Ex-1004, 2:32–36. A POSA would have understood that this user record would have included the user’s cell phone number and would have been stored in a database. Ex-1003, ¶¶ 161–162. Further, Sormunen discloses: “The using of the service may be initiated almost immediately after a subscription request has been sent, because transmission of user information is conducted in enciphered, electronic form and the receiver can be recognized in order to prevent abuse.” Ex-1004, 5:11–16. Thus, a POSA would have understood that recognizing the receiver for reply message 6 would have inherently required associating the paging terminal/mobile station with the user. Thus, Sormunen discloses that “associating a user with a personal communication device possessed by the user.” Ex-1003, ¶¶ 161–162.

Sormunen further discloses the use of “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 phone number.” Ex-1004, 4:30–34. Sormunen discloses that “[a] cellular system, such as the GSM system, is a mobile communication system in which a cellular network is used” (*said personal communication device in communication over a second network, wherein said second network is a cell phone network*). Ex-1004, 5:1–3. As disclosed by Sormunen, the cellular network is different from the first secure computer network. Ex-1003, ¶¶ 163–164. The mobile station communicates over a cellular network (e.g., GSM) with the paging service provider 4 (or short message service center), Ex-1004, 5:38–6:20; *see also* Ex-1004, 8:19–22 (“Transmission of short messages between the paging terminal 3 and the short message service center 4 is made preferably at least in part in a wireless manner, for example, by using a mobile communication network.”); Ex-1003, ¶ 163. Access terminal (or data processor) 8 can communicate with protected service 1 over “a modem connection to a wireline telecommunication network.” Ex-1004, 8:5–7. Thus, the cellular network is different than the wireline telecommunication network disclosed by Sormunen used to gain access to the protected service. Ex-1003, ¶¶ 163–164. This specifically addresses the examiner’s reason for allowance. Ex-1002, 294–295; Ex-1003, ¶ 163.

Sormunen discloses the paging terminal/mobile terminal in communication over a cell phone network (green) that is different than the first secure computer network (orange). Ex-1003, ¶ 164.

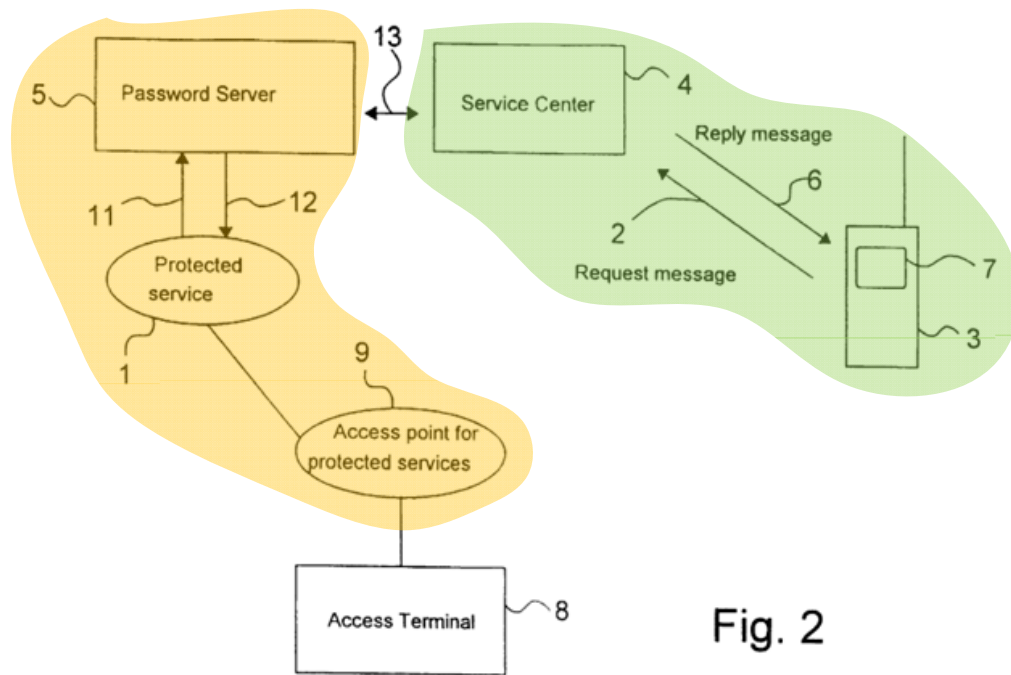


Fig. 2

Ex. 1004, FIG. 2 (annotated).

- c. **receiving a request from the user for a token via the personal communication device, over the second network;**

Sormunen in view of Perlman teaches or suggests “receiving a request from the user for a token via the personal communication device, over the second network.” Sormunen discloses “receiving a request from the user for a token via the personal communication device over the second network.” As underlined below in annotated Fig. 2 of Sormunen, Sormunen discloses receiving request

message 2 (*receiving a request from the user*) via a paging terminal/mobile terminal (*personal communication device*) over the cell phone network (second network). Ex-1003, ¶¶ 166–166.

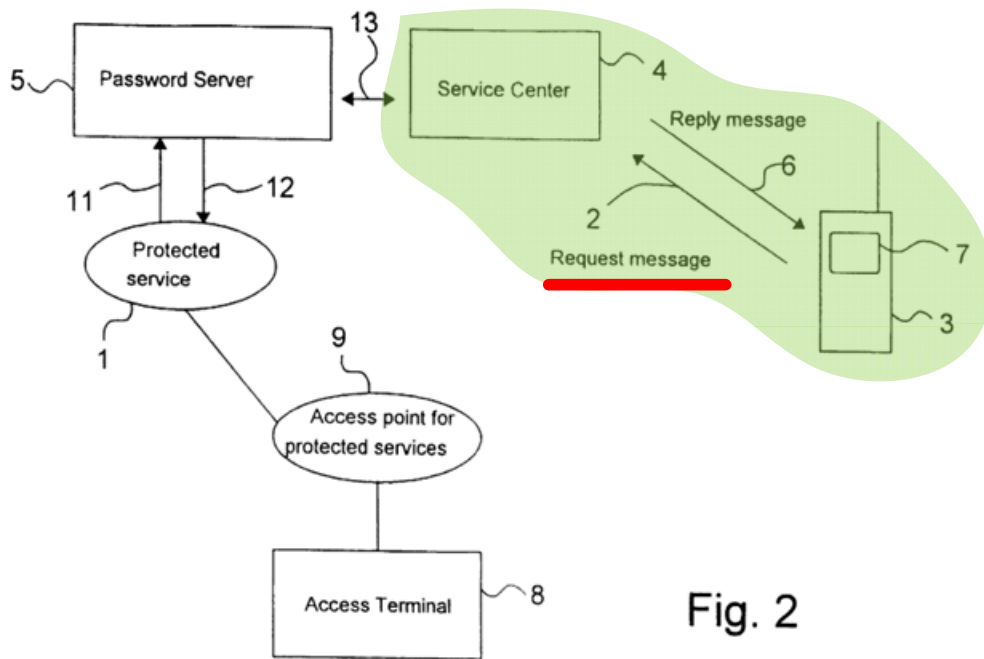


Fig. 2

Ex. 1004, FIG. 2 (annotated).

Sormunen discloses: “The short message 2 includes a password request and possibly also a subscription request for a new user.” Ex-1004, 5:38–6:2. A POSA would understand that upon account creation, a password (string) could be provided to the user. A POSA would understand that this password would have the same role or function as the claimed “passcode.” Ex-1003, ¶ 167.

Sormunen also discloses requesting and receiving a new PIN via a personal communication device. Ex-1004, 9:26–37; Ex-1003, ¶ 168. A POSA would have

understood that a PIN is also one user specific authentication data disclosed in Sormunen, and that Sormunen discloses requesting and receiving them over a cell phone network. Ex-1003, ¶ 168; Ex-1004, 9:26–37. Further, as reflected in the state of the art, a POSA would appreciate that a password and a PIN could be used together for greater security. Ex-1003, ¶ 168. For example, they could be used together to address the known problem of a third party obtaining (e.g., guessing, intercepting) one item of user specific authentication data. *Id.* A POSA would have found it obvious for the new password to be combination of the known password (passcode) and the PIN (token) generated in response to the request. *Id.*

Further, Perlman teaches using a character string generated by an authentication token to augment an existing character string. Ex-1003, ¶ 169; Ex-1005, 4:38–64; Ex-1005, 8:49–9:9; Ex-1005, 11:8–20. Thus, a POSA would have appreciated that Perlman teaches augmenting a known character string using a requested character string unknown to the user, at least at that point (*token*). Ex-1003, ¶ 169.

- d. 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;**

Sormunen in view of Perlman teaches “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.” Sormunen discloses: “The short message 2 includes a password request and possibly also a subscription request for a new user.” Ex-1004, 5:38–6:2. Sormunen also discloses that this request could be for a new PIN. Ex-1004, 9:34–37; Ex-1003, ¶¶ 171–172.

Sormunen discloses that upon account setup, the new user may have a password assigned or selected. Ex-1004, 3:25–32. A POSA would have understood that this initial password teaches the claimed “passcode.” Ex-1003, ¶ 173. A POSA would have appreciated that it is a string known to the user and known to the system. *Id.* However, a POSA would understand that security can be improved by augmenting the string known to the user with a PIN to create a more secure password. *Id.* Thus, a POSA would know from Sormunen to combine the disclosed initial password with the new PIN to create a new password. *Id.* A POSA would understand that a PIN would commonly be generated by known techniques to produce a randomized string. *Id.*

Perlman discloses generating a character string and “communicat[ing] it to a local device (e.g., a work station) where it can be modified using a predetermined function to produce a result (i.e., a second character string).” Ex-1005, 4:38–64; Ex-1005, 8:49–9:9; Ex-1005, 11:8–20; Ex-1003, ¶ 174. The resultant “second character string” is communicated to a remote device for authentication. Ex-1005,

4:38–64; Ex-1005, 8:49–9:9; Ex-1005, 11:8–20; Ex-1003, ¶ 174. A POSA would have understood that concatenation was a predetermined function for modifying a first character string with another character string to produce a second character string. Ex-1003, ¶ 174.

A POSA would have appreciated that Perlman teaches concatenating a known secret character string with a generated character string provided through a token. Ex-1003, ¶ 175. A POSA would have appreciated that the resulting character string could be used more securely as a password than the original known secret character string. *Id.* Thus, a POSA would have been motivated to combine the teachings of Perlman with Sormunen. *Id.* The original password set for the user (including one proposed by the user) could be augmented by concatenating it with a generated PIN. *Id.* A POSA would appreciate that, according to the teachings of Perlman, this predetermined function (concatenation) would be known to the password server. Thus, the password server generates a PIN, and then sets the password as the concatenation of the preexisting or initial password and the PIN, which may be randomized according to techniques known to POSAs. *Id.* The PIN (user authentication information) would then be transmitted to the user via the user’s paging terminal/mobile station. *Id.*

Sormunen and Perlman also disclose that the token is “not known to the user.” Perlman, for example, discloses that “the workstation can read the character

string automatically from the authentication token after the user has entered a PIN into the workstation.” Ex-1005, 8:60–62. Similarly, Sormunen discloses that a “data processor,” such as access terminal 8, can be “coupled to a mobile station.” Ex-1004, 6:11–12. Thus, a POSA would understand that Sormunen and Perlman disclose that a token may not be not known the user even after the new password is created. Ex-1003, ¶ 176. However, it could also be shown to the user after receipt via display means 7 on the paging terminal 3/mobile station. *Id.*; Ex-1004, 7:4–6 (“The reply message 6 arrived to the paging terminal 3 can be shown to the user for example by display means 7 of a mobile station used as a paging terminal.”).

e. setting a password associated with the user to be the new password;

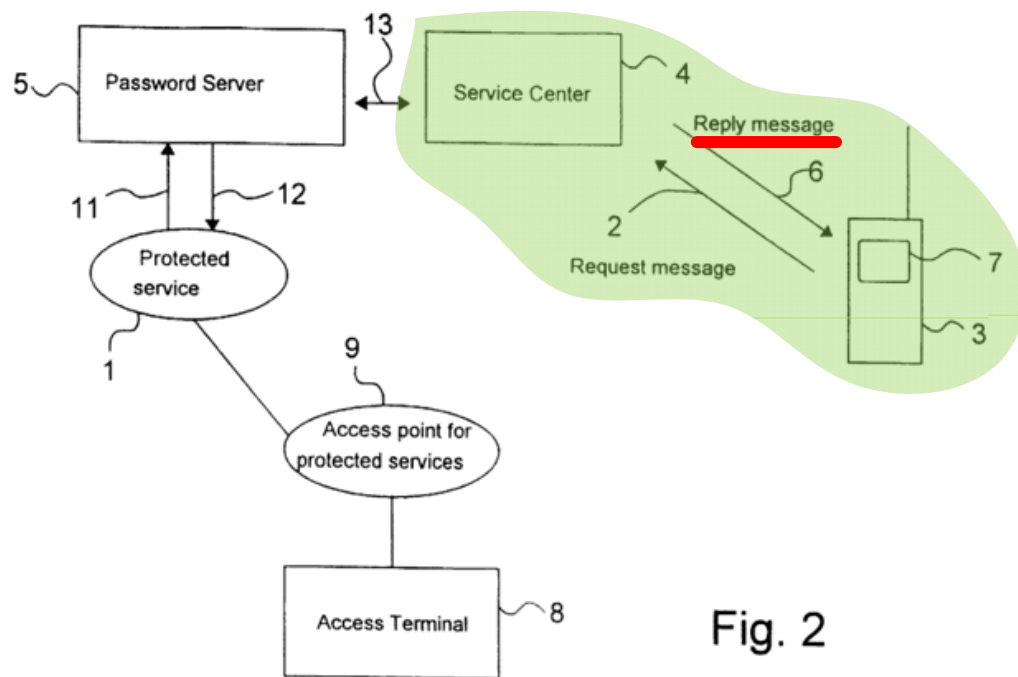
Sormunen and Perlman teach “setting a password associated with the user to be the new password.” The password server of Sormunen is disclosed as setting passwords associated with users. Ex-1004, 5:38–6:2, 6:22–30. A POSA would appreciate that the password server would set the password associated with the user as the preexisting password augmented by the generated PIN according to a predetermined function, as taught by Perlman. Ex-1005, 4:38–64; Ex-1005, 8:49–9:9; Ex-1005, 11:8–20; Ex-1003, ¶ 177.

f. activating access the user account on the first secure computer network;

Sormunen disclose this step. Ex-1003, ¶ 178. Sormunen discloses: “The short message 2 includes a password request and possibly also a subscription request for a new user.” Ex-1004, 5:38–6:2. “The using of the service may be initiated almost immediately after a subscription request has been sent, because transmission of user information is conducted in enciphered, electronic form and the receiver can be recognized in order to prevent abuse.” Ex-1004, 5:11–16. The user information may include a user name. Thus, Sormunen discloses that the user has an account on the information service/protected service (*first secure computer network*). Ex-1003, ¶ 178.

g. transmitting the token to the personal communication device;

Sormunen teaches or suggests “transmitting the token to the personal communication device.” Ex-1003, ¶ 179. Sormunen discloses: “The password server 5 transmits the password and/or the user name to the short message service center 4, which forms according to the data a reply message 6, which is sent to the paging terminal 3 preferably in enciphered form.” Ex-1004, 6:35–38. Reply message 6 is underlined in red in annotated Fig. 2 of Sormunen below.



Ex. 1004, FIG. 2 (annotated).

h. receiving the password from the user via the first secure computer network; and

The combination of Sormunen and Perlman discloses “receiving the password from the user via the first secure computer network.” As shown in annotated Fig. 2 of Sormunen below, Sormunen discloses receiving the password from the user via the first secure computer network (orange). Ex-1003, ¶ 180.

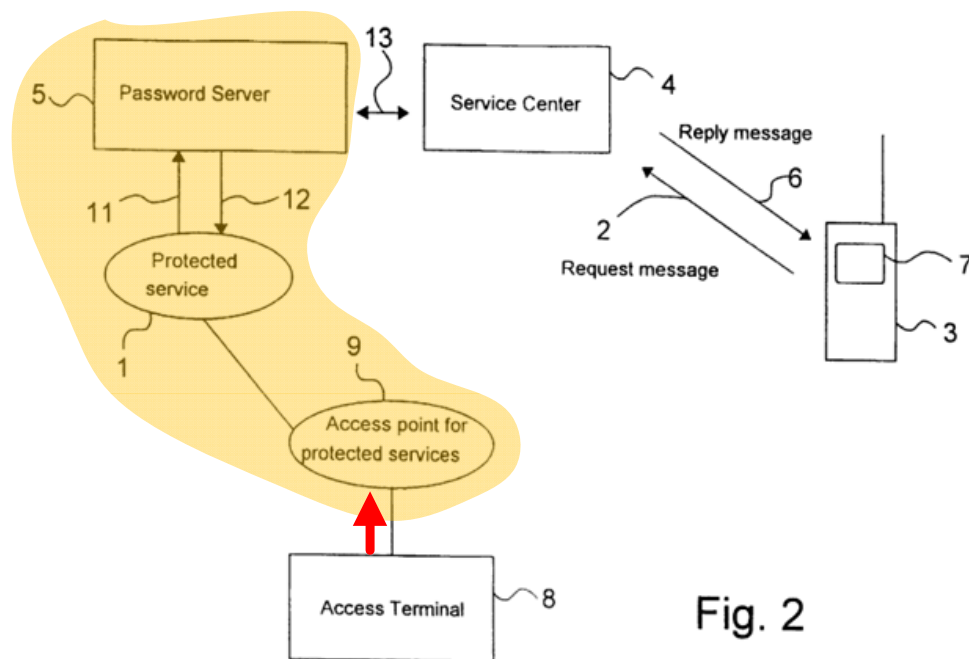


Fig. 2

Ex. 1004, FIG. 2 (annotated).

- i. **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.**

Sormunen in view of Perlman teaches 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. Ex-1003, ¶ 181.

Sormunen discloses that when the password submitted through access terminal 8 matches the one in the system, the user is given access (access to the account in response to the password). Ex-1004, 7:9–20 (“After the user has given

his or her user name and the valid password, the verification service 9 transmits the given data to the service 1, which sends a check request 11 of the user name and the password to password server 5. The password server 5 examines the data and communicates in a reply message 12 whether the user name and the password are given correctly. If the data is correct, the user has a data transmission connection from the data processor 8 to the service 1.”). Further, Sormunen discloses that passwords are only valid for a predetermined amount of time, so access will be denied if not received within that period (*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*). Ex-1004, 2:13 (“[A] periodical password valid for a predefined period of time.”); Ex-1004, 5:16–18 (“A further advantage of the fast data transmission is that the validity of passwords can be shortened remarkably and security may thus be improved”). Thus, even if the password is correct, the user would not be able to gain access if the validity period has ended (*said user account is not accessible through any password, via said first secure computer network*). Ex-1003, ¶ 182.

2. Claim 2: The method of claim 1, wherein the new password is generated by concatenating the token and the passcode.

Claim 2 is obvious over Sormunen in view of Perlman. Claim 2 provides that the password generated by claim 1 is generated by “concatenating the token

and the passcode.” Combining the initial/preexisting password (passcode) and generated PIN (token) by concatenating them would have been obvious to a POSA. Ex-1003, ¶ 181. It would have been common sense to combine them by concatenation. Ex-1003, ¶¶ 183–186. Concatenation was a basic function performed on strings, easy for a POSA to use, and was in widespread use as of March 6, 2000. Ex-1003, ¶ 185; *see also* Ex-1003, ¶¶ 89–102; Ex-1011; Ex-1012; Ex-1013; Ex-1014.

Even if it was not common sense, as explained above in Section VI.B.1.d, Perlman teaches concatenating a string generated by a token with a preexisting secret string to produce a more secure password. Ex-1003, ¶ 184.

3. Claim 3: The method of claim 1, wherein the personal communication device is a mobile phone.

Sormunen discloses “wherein the personal communication device is a mobile phone.” Sormunen discloses a paging terminal (paging terminal 3 in Fig. 2), which may be a “mobile station.” Ex-1004, 5:33–38 (“the user of the service sends a short message 2 from the paging terminal 3, such as a mobile station.”) This is highlighted in blue in Fig. 2 of Sormunen below.

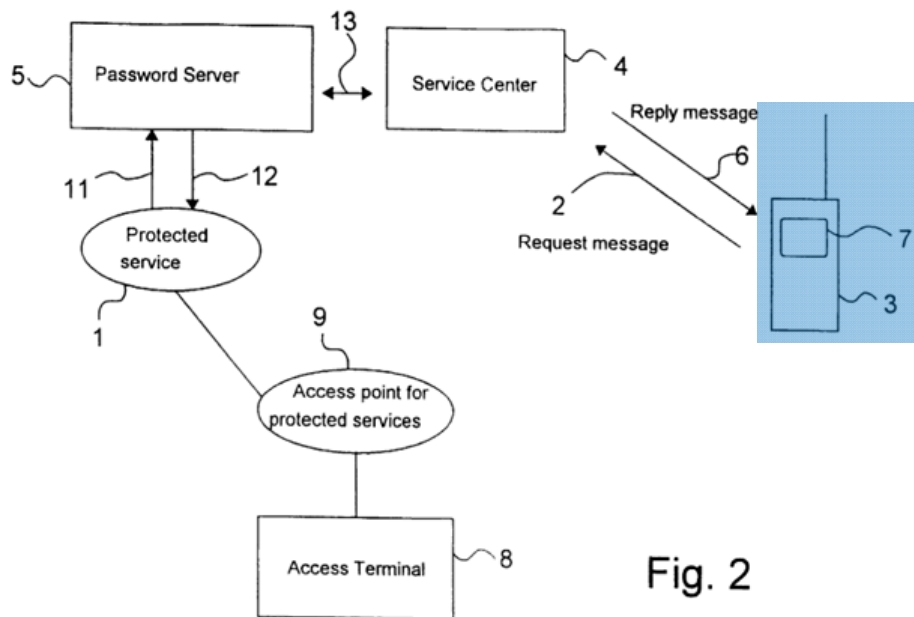


Fig. 2

Ex. 1004, FIG. 2 (annotated).

The mobile station may communicate via SMS over a cellular network. Ex-1004, 5:38–6:20. Thus, Sormunen discloses “the personal communication device is a mobile phone.” Ex-1003, ¶¶ 187–188.

4. Claim 4: The method of claim 1, wherein the personal communication device is a pager.

Sormunen discloses “wherein the personal communication device is a pager.” Sormunen discloses “paging terminal 3,” which may be, “for example a paging device or the like . . . whereby the method of transmitting the reply message to the paging device depends for example on the paging system used.” Ex-1004, 8:33–35. Further, paging service center 4 is also disclosed as being “for example, a paging network controller or a wireless messaging switch.” Ex-1004, 8:36–37.

Thus, Sormunen discloses “the personal communication device is a pager.” Ex-1003, ¶ 189.

5. Claim 5

Claims 5–7 overlap with claim 1. The discussion above regarding claim 1 is also applicable below to the corresponding system elements.

a. A user authentication system comprising:

If the preamble is limiting, it is disclosed by Sormunen. Ex-1003, ¶ 191. Sormunen discloses “a method and system for obtaining at least one item of user specific authentication data, such as a password and/or a user name.” Ex-1004, 1:3–5. Sormunen discusses the use of “information services,” which can be connected to via a “data transmission connection” over a “telecommunication network or a mobile communication network.” Ex-1004, 1:8–13. To use the information service, “usually user specific authentication data is required, for example a user name and password.” Ex-1004, 1:14–15. The user name and password “enable the information service provider to control the user using the information service” and “prevent unauthorized use of the information service.” Ex-1004, 1:17–22. Thus, Sormunen discloses a “user authentication system.”

This is further reflected in Fig. 2 of Sormunen, reproduced below, which “shows a method for transmitting a user name and passwords according to a

preferred embodiment of the invention.” Ex-1004, 5:26–27.

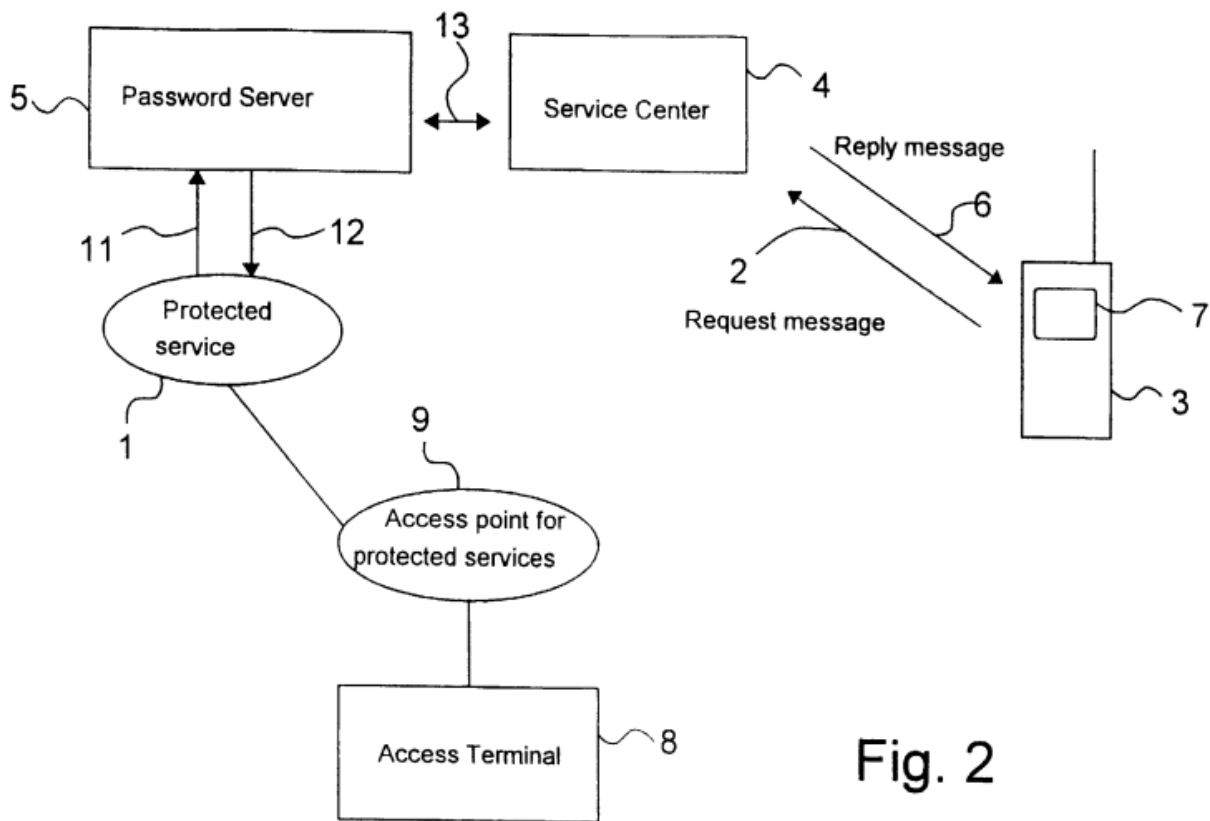


Fig. 2

Ex. 1004, FIG. 2.

b. a computer processor;

Sormunen teaches “a computer processor.” A POSA would understand that the password server of Sormunen necessarily includes a computer processor. Ex-1003, ¶ 194. For example, Sormunen discloses: “The service block 1, the password server block 5 and the verification service block 9 shown in the block diagram of Fig. 2, can be placed for example in the mainframe of the service provider or the like, or they can be separate data processors between which data transmission

connections are formed.” Ex-1004, 8:9–13. A POSA would understand that the password server would not function in the way disclosed by Sormunen (or at all) without a computer processor. Ex-1003, ¶ 194.

- c. 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;**

This element is taught by Sormunen and Perlman as discussed above regarding claim 1(a). Ex-1003, ¶¶ 195–198.

- d. 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;**

This element is taught by Sormunen and Perlman as discussed above with respect to claim 1(d) and 1(e). Ex-1003, ¶ 199. Sormunen discloses a “password server.” A POSA would know that the password server would necessarily have a computer processor and execute its claimed functions on it. Ex-1003, ¶ 199.

- e. a communication module configured to transmit the token to the personal communication device through the cell phone network; and**

This element is taught by Sormunen and Perlman as discussed above with respect to claim 1(g). Ex-1003, ¶¶ 201–202.

- f. 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, 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.**

This element is taught by Sormunen and Perlman as discussed with respect to claim 1(a), (b), (f), (h), and (i). Ex-1003, ¶¶ 203–206.

- 6. Claim 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.**

This limitation is taught Sormunen in view of Perlman as discussed above regarding claim 1(c), 1(d), and 1(e). Ex-1003, ¶ 207.

- 7. Claim 7: The system of claim 6, wherein the request is transmitted by the user through the personal communication device.**

Sormunen teaches this limitation as discussed above with respect to claim 1(c). Ex-1003, ¶ 209.

VII. INSTITUTION DISCRETION

The Board should not decline institution under 35 U.S.C. § 325(d) or § 314(a).

A. *General Plastic* Factors Favor Petitioner

Experian respectfully submits there is no basis for discretionary denial under 35 U.S.C. § 325(d).

The *General Plastic* factors favor institution. *General Plastic Indus. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 at 15–16 (P.T.A.B. Sept. 6, 2017) (precedential as to Section II.B.4.i). The first factor is “whether the same petitioner previously filed a petition directed to the same claims of the same patent.” *Id.* at 16. Factors two through five assume the answer is “yes.” *Id.* The sixth factor is “the finite resources of the Board” and the seventh factor is “the requirement under 35 U.S.C. § 316(a)(11) to issue a final determination not later than 1 year after the date on which the Director notices institution of review.” *Id.* All factors favor Petitioner.

Petitioner has not filed or been a party to any prior petitions seeking review of any claims of the ’658 Patent. *Unified Patents, LLC v. Dynapass IP Holdings LLC*, IPR2023-00425, Paper 9 (P.T.A.B. July 18, 2023) (instituting *inter partes* review of claims 1 and 3–6 of the ’658 Patent); *JPMorgan Chase & Co. v. Dynapass IP Holdings LLC*, IPR2023-01331, Paper 1 (P.T.A.B. Aug. 16, 2023)

(pending institution on the same grounds as and seeking joinder with *Unified Patents*); *Bank of America, NA v. Dynapass IP Holdings LLC*, IPR2023-00367, Paper 9 (P.T.A.B. July 18, 2023) (denying institution of *inter partes* review). Petitioner is not a party to the ongoing proceedings, and was not a party to the proceeding where institution was denied. As a result, factors one through five favor Petitioner.

Factors six and seven also favor Petitioner. The instant Petition presents meritorious grounds for review of all seven claims of the '658 Patent. As discussed above, Sormunen was not before the examiner and directly addresses the examiner's reason for allowance. While Perlman was cited as relevant in an international search report and information disclosure statement, Ex-1002, 177 and 222, its citation does not support discretionary denial given the lack of arguments concerning it and its use in the instant petition in combination with Sormunen.

The *Unified Patents* proceeding includes two grounds: Veneklas in view of Jonsson (claim 5), and Kew in view of Sormunen (claims 1 and 3–6). *Unified Patents*, IPR2023-00425, Paper 9 at 7. Kew in view of Sormunen was not considered on the merits at the institution decision phase because review was found to be properly instituted on the first ground. *Id.* at 25. Thus, the *Unified Patents* proceeding involves a different combination of the teachings of Sormunen (as a secondary reference) with a reference not raised in this Petition.

There is no evidence that the requested review would strain the resources of the Board, and there is no indication a final written decision would not issue within the statutory period. Accordingly, the *General Plastic* factors favor Experian.

B. *Fintiv* Factors Favor Petitioner

Experian respectfully submits that no basis exists under 35 U.S.C. § 314(a) for discretionary denial. The Board “will not discretionarily deny institution . . . where a petitioner presents a [*Sotera*] stipulation.” USPTO Director Vidal, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (Memorandum, June 21, 2022) at 3, *available at* <https://tinyurl.com/a6x9xnvj> (citing *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (P.T.A.B. Dec. 1, 2020) (precedential as to § II.A)). Petitioner is presenting a *Sotera* stipulation. Ex-1021. The Board need not address additional considerations in view of the stipulation. However, they also do not favor denial.

Factors concerning the Board’s discretion are provided by *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020) (precedential). These are discussed below.

1. whether a stay has been granted or may be granted if a proceeding is instituted

The Court has not granted or denied a stay. Further, there is no evidence that a stay would be denied if review is instituted. Thus, this factor is neutral.

2. proximity of the court's trial date to the Board's projected statutory deadline for a final written decision

Trial is scheduled to begin October 7, 2024. Ex-1017. The projected deadline for the final written decision is March 28, 2025. However, the trial date is subject to change. Further, the trial date is the same for Experian and several other defendants² whose cases have been consolidated for pretrial matters only. Ex-1020. Thus, there is some chance the district court trial will not proceed before a final written decision in this proceeding. Accordingly, this factor is neutral.

3. investment in the parallel proceeding by the court and the parties

This factor favors institution. The case is currently in fact discovery and no substantive orders have been issued. Further, no depositions have been taken, no subpoenas issued, and Patent Owner has only just served its first set of interrogatories (i.e., on September 27, 2023).

² Amazon.com, Inc., The Charles Schwab Corporation, Charles Schwab Bank, SSB, Simmons Bank, and Simmons First National Corporation.

Under the current schedule, the deadline for substantial completion of document production is March 13, 2024, and fact discovery is scheduled to end May 20, 2024. Ex-1017. Expert disclosures are not due until May 20, 2024. *Id.* Claim construction has not yet begun. The claim construction hearing is scheduled for May 15, 2024. *Id.* The parties are not scheduled to even exchange proposed claim terms until December 20, 2023. *Id.* Thus, this factor favors institution.

4. overlap between issues raised in the petition and in the parallel proceeding

Petitioner is alleged to infringe claims 1–3 and 5–7 of the ’658 Patent in the parallel district court proceeding. Ex-1019. The Petition challenges claims 1–7, thus, thus there is a difference between what claims are being asserted claims and what claims are being challenged. Regardless, as mentioned above, Petitioner is offering a *Sotera* stipulation. Ex-1021. Accordingly, this factor favors Petitioner.

5. whether the petitioner and the defendant in the parallel proceeding are the same party

Petitioner is the defendant and Patent Owner is the plaintiff in the district court litigation.³ Thus, this factor does not favor Petitioner.

³ Patent Owner erroneously identified Petitioner as “Experian Information Services, Inc.” in Patent Owner’s Complaint. *See* Ex-1018.

6. other circumstances that impact the Board’s exercise of discretion, including the merits

This factor weighs in favor of institution. Petitioner has filed the petition within the 12-month statutory period and has, as explained herein, presented compelling grounds for the unpatentability of claims 1–7 of the ’658 Patent that would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence. Petitioner presents analogous prior art (Sormunen) that directly addresses the examiner’s reason for allowance of the claims of the ’658 Patent and that was not considered or cited by the examiner. Accordingly, this factor favors Petitioner because Petitioner presents a “compelling, meritorious” challenge.

In sum, the relatively low level of investment in the parallel district court proceeding at this stage, Petitioner’s *Sotera* stipulation, and the strength of the challenge presented all favor declining to exercise discretion under 35 U.S.C. § 314(a) to deny the Petition.

VIII. MANDATORY NOTICES

Petitioner provides the following mandatory notices under 37 C.F.R. § 42.8.

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

The real party-in-interest is Experian Information Solutions, Inc.

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

The ’658 Patent is at issue in the following matters:

Unified Patents, LLC v. Dynapass IP Holdings, LLC,

IPR2023-00425 (P.T.A.B. filed Jan. 6, 2023)

JPMorgan Chase & Co. v. Dynapass IP Holdings, LLC,

IPR2023-01331 (P.T.A.B. filed Aug. 16, 2023)

Dynapass IP Holdings, LLC v. Amazon.com Inc.,

No. 2:23-cv-00063 (E.D. Tex. filed Feb. 20, 2023)

Dynapass IP Holdings, LLC v. The Charles Schwab Corporation,

No. 2:23-cv-00064 (E.D. Tex. filed Feb. 20, 2023)

Dynapass IP Holdings, LLC v. Experian Information Services, Inc.,

No. 2:23-cv-00066 (E.D. Tex. filed Feb. 20, 2023)

Dynapass IP Holdings, LLC v. Simmons First National Corporation,

No. 2:23-cv-00068 (E.D. Tex. filed Feb. 20, 2023)

Dynapass IP Holdings, LLC v. Bank of America Corporation,

No. 2:22-cv-000210 (E.D. Tex. filed June 17, 2022)

Dynapass IP Holdings, LLC v. BOKF, National Association,

No. 2:22-cv-000211 (E.D. Tex. filed June 17, 2022)

Dynapass IP Holdings, LLC v. JPMorgan Chase & Co.,

No. 2:22-cv-000212 (E.D. Tex. filed June 17, 2022)

Dynapass IP Holdings, LLC v. PNC Financial Services Group, Inc.,

No. 2:22-cv-000214 (E.D. Tex. filed June 17, 2022)

Dynapass IP Holdings, LLC v. Truist Financial Corporation,

No. 2:22-cv-000216 (E.D. Tex. filed June 17, 2022)

Dynapass IP Holdings, LLC v. Wells Fargo & Company,

No. 2:22-cv-000217 (E.D. Tex. filed June 17, 2022)

Jack Henry & Associates, Inc. v. Dynapass IP Holdings LLC,

No. 1:23-cv-00388 (D. Del. filed Apr. 5, 2023)

C. Lead and Back-Up Counsel and Service Information

Lead Counsel	Backup Counsel
James B. Hatten, Reg. No. 74,235 Telephone: (404) 256-8242 Facsimile: (404) 459-5734 jhatten@bakerlaw.com BAKER & HOSTETLER LLP 1170 Peachtree Street NE, Suite 2400 Atlanta, GA 30309-7676	Glenn D. Richeson, Reg. No. 73,780 Telephone: (404) 946-9835 Facsimile: (404) 459-5734 gricheson@bakerlaw.com BAKER & HOSTETLER LLP 1170 Peachtree Street NE, Suite 2400 Atlanta, GA 30309-7676

Please direct all correspondence to lead and back-up counsel at the above addresses. Petitioner consents to electronic service at the email addresses above.

IX. Payment of Fees Pursuant to 37 C.F.R. § 42.103

Petitioner requests review of seven claims. The Director may charge the section 42.15(a)(1) fee and any additional fees in connection with this Petition to Deposit Account No. 502036.

Petition for *Inter Partes* Review of U.S. Patent No. 6,993,658
IPR2023-01406

Date: September 27, 2023

Respectfully submitted,

/James B. Hatten/

James B. Hatten (Reg. No. 74,235)
jhatten@bakerlaw.com
(404) 256-8242
Glenn Richeson (Reg. No. 73,780)
gricheson@bakerlaw.com
(404) 946-9835
BAKER & HOSTETLER LLP
1170 Peachtree Street NE, Suite 2400
Atlanta, GA 30309-7676

*Counsel for Experian Information
Solutions, Inc.*

CERTIFICATE OF COMPLIANCE

This Petition complies with the word count limitation of 37 C.F.R. § 42.24(a)(1) because, according to the word processing system used to prepare this document, the Petition contains 10,650 words, excluding the cover page, signature block, the exhibit list, and the parts of the Petition exempted by 37 C.F.R. § 42.24(a)(1).

/James B. Hatten/

James B. Hatten (Reg. No. 74,235)

CERTIFICATE OF SERVICE

In compliance with 37 C.F.R. §§ 42.105 and 42.6(e), the undersigned hereby certifies that a copy of this Petition, Exhibits 1001–1021, and Petitioner’s Power of Attorney and Designation of Lead and Backup Counsel, were served on the 28th day of September, 2023, by Priority Mail Express® directed to the Patent Owner at the correspondence address of record:

DynaPass Inc.
PO Box 11510
Costa Mesa, CA
United States

A courtesy copy was also served by electronic mail on Patent Owner’s counsel of record in District Court Litigation:

John Wittenzellner (johnw@wsltrial.com)
Todd Landis (tlandis@wsltrial.com)
Michael J. Fagan, Jr. (mfagan@wsltrial.com)
Fred Williams (fwilliams@wsltrial.com)
Williams, Simons, and Landis, PLLC
dynapasscounselwsl@wsltrial.com

/James B. Hatten/

James B. Hatten (Reg. No. 74,235)