8406150

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

August 21, 2023

THIS IS TO CERTIFY THAT ANNEXED IS A TRUE COPY FROM THE RECORDS OF THIS OFFICE OF THE FILE WRAPPER AND CONTENTS OF:

APPLICATION NUMBER: *09/519,829*
FILING DATE: *March 06, 2000*
PATENT NUMBER: *6993658*
ISSUE DATE: *January 31, 2006*

Certified by

Performing the Functions and Duties of the
Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

EXPERIAN EXHIBIT 1002
IPR2023-01406

03/06/00 jc784 U.S. PTO

03-0700

4

PATENT

Attorney Docket No. APRILS.001A
Date: March 6, 2000
Page 1

jc530 U.S. PTO 09/519829 03/06/00

ASSISTANT COMMISSIONER FOR PATENTS

WASHINGTON, D.C. 20231

ATTENTION: BOX PATENT APPLICATION

Sir:

Transmitted herewith for filing is the patent application of

Inventors: **Sten-Olov Engberg and Ake Jonsson**

For: **USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION**

Enclosed are:

(X) A Specification in 21 pages

(X) 11 sheets of drawing.

(X) An Information Disclosure Statement.

(X) A PTO Form 1449 with three (3) references.

(X) A return prepaid postcard.

CLAIMS AS FILED

FOR	NUMBER FILED	NUMBER EXTRA	RATE	FEE
Basic Fee			$690	$690.00
Total Claims	27 - 20 =	7 ×	$18	$126.00
Independent Claims	4 - 3 =	1 ×	$78	$78.00
If application contains any multiple dependent claims(s), then add			$260	$0

FILING FEE TO BE PAID AT A LATER DATE $894.00

(X) Please use Customer No. 20,995 for the correspondence address.

Jerry T. Sewell
Registration No. 31,567
Attorney of Record

JTS-4508.DOC:ke
20000306

KNOBBE, MARTENS, OLSON & BEAR, LLP
620 NEWPORT CENTER DR 16TH FLOOR NEWPORT BEACH, CA 92660
(949) 760-0404 FAX (949) 760-9502

INTELLECTUAL PROPERTY LAW

KNOBBE, MARTENS, OLSON & BEAR

A LIMITED LIABILITY PARTNERSHIP INCLUDING
PROFESSIONAL CORPORATIONS

PATENT, TRADEMARK AND COPYRIGHT CAUSES

620 NEWPORT CENTER DRIVE

SIXTEENTH FLOOR

NEWPORT BEACH, CALIFORNIA 92660-8016

(949) 760-0404

FAX (949) 760-9502

INTERNET: WWW.KMOB.COM

LOUIS J. KNOBBE*
DON W. MARTENS*
GORDON H. OLSON*
JAMES B. BEAR
DARRELL L. OLSON*
WILLIAM B. BUNKER
WILLIAM H. NIEMAN
ARTHUR S. ROSE
JAMES F. LESNIAK
NED A. ISRAELSEN
DREW S. HAMILTON
JERRY T. SEWELL
JOHN B. SGANGA, JR
EDWARD A. SCHLATTER
GERARD VON HOFFMANN
JOSEPH R. RE
CATHERINE J. HOLLAND
JOHN M. CARSON
KAREN VOGEL WEIL
ANDREW H. SIMPSON
JEFFREY L. VAN HOOSEAR
DANIEL E. ALTMAN
MARGUERITE L. GUNN
STEPHEN C. JENSEN
VITO A. CANUSO III
WILLIAM H. SHREVE
LYNDA J. ZADRA-SYMES†
STEVEN J. NATAUPSKY
PAUL A. STEWART
JOSEPH F. JENNINGS
CRAIG S. SUMMERS
ANNEMARIE KAISER
BRENTON R. BABCOCK

THOMAS F. SMEGAL, JR
MICHAEL H. TRENHOLM
DIANE M. REED
JONATHAN A. BARNEY
RONALD J. SCHOENBAUM
JOHN R. KING
FREDERICK S. BERRETTA
NANCY WAYS VENSKO
JOHN P. GIEZENTANNER
ADEEL S. AKHTAR
GINGER R. DREGER
THOMAS R. ARNO
DAVID N. WEISS
DANIEL HART, PH.D.
DOUGLAS G. MUEHLHAUSER
LORI LEE YAMATO
MICHAEL K. FRIEDLAND
STEPHEN M. LOBBIN
STACEY R. HALPERN
DALE C. HUNT, PH.D.
LEE W. HENDERSON, PH.D.
DEBORAH S. SHEPHERD
RICHARD E. CAMPBELL
MARK M. ABUMERI
JON W. GURKA
ERIC M. NELSON
ALEXANDER C. CHEN
MARK R. BENEDICT, PH.D.
PAUL N. CONOVER
ROBERT J. ROBY
SABING H. LEE
KAROLINE A. DELANEY
JOHN W. HOLCOMB

JAMES J. MULLEN, III, PH.D.
JOSEPH S. CIANFRANI
JOSEPH M. REISMAN, PH.D.
WILLIAM R. ZIMMERMAN
GLEN L. NUTTALL
ERIC S. FURMAN, PH.D.
DO TE KIM
TIRZAH ABE LOWE
GEOFFREY Y. IIDA
ALEXANDER S. FRANCO
SANJIVPAL S. GILL
SUSAN M. MOSS
JAMES W. HILL, M.D.
ROSE M. THIESSEN, PH.D.
MICHAEL L. FULLER
MICHAEL A. GUILIANA
MARK J. KERTZ
RABINDER N. NARULA
BRUCE S. ITCHKAWITZ, PH.D.
PETER M. MIDGLEY
THOMAS S. MCCLENAHAN
MICHAEL S. OKAMOTO
JOHN M. GROVER
MALLARY K. MCCARTHY
IRFAN A. LATEEF
AMY C. CHRISTENSEN
SHARON S. NG
MARK J. GALLAGHER, PH.D.
DAVID G. JANKOWSKI, PH.D.
BRIAN C. HORNE
PAYSON J. LEMEILLEUR

OF COUNSEL
JERRY R. SEILER

JAPANESE PATENT ATTY
KATSUHIRO ARAI**

EUROPEAN PATENT ATTY
MARTIN HELLEBRANDT

KOREAN PATENT ATTY
MINCHEOL KIM

SCIENTISTS & ENGINEERS
(NON-LAWYERS)

RAIMOND J. SALENIEKS**
NEIL S. BARTFELD, PH.D.**
DANIEL E. JOHNSON, PH.D.**
JEFFERY KOEPKE, PH.D.
KHURRAM RAHMAN, PH.D.
JENNIFER A. HAYNES, PH.D.
BRENDAN P. O'NEILL, PH.D.
THOMAS Y. NAGATA
ALAN C. GORDON
LINDA H. LIU
MICHAEL J. HOLIHAN
YASHWANT VAISHNAV, PH.D.
MEGUMI TANAKA

* A PROFESSIONAL CORPORATION
† ALSO BARRISTER AT LAW (U.K.)
** U.S. PATENT AGENT

Assistant Commissioner for Patents
Washington, D.C. 20231

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

Attorney Docket No.	:	APRILS.001A
Applicant(s)	:	Sten-Olov Engberg, et al.
For	:	USE OF PERSONAL COMMUNICATION DEVICE FOR USER AUTHENTICATION
Attorney	:	Jerry T. Sewell
"Express Mail" Mailing Label No.	:	EL 103 698 371 US
Date of Deposit	:	March 6, 2000

I hereby certify that the accompanying

Transmittal in Duplicate; Specification in 21 pages; 11 sheets of drawings; Information Disclosure Statement, PTO Form 1449 with three (3) references; Return Prepaid Postcard

are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and are addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Donald King

JTS-4507.DOC:ke
20000306

201 CALIFORNIA STREET
SUITE 1150
SAN FRANCISCO, CALIFORNIA 94111
(415) 954-4114
FAX (415) 954-4111

501 WEST BROADWAY
SUITE 1400
SAN DIEGO, CALIFORNIA 92101
(619) 235-8550
FAX (619) 235-0176

3801 UNIVERSITY AVENUE
SUITE 710
RIVERSIDE, CALIFORNIA 92501
(909) 781-9231
FAX (909) 781-4507

1875 CENTURY PARK EAST
SUITE 600
LOS ANGELES, CALIFORNIA 90067
(310) 407-5484
FAX (310) 407-5485

USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION

Background of the Invention

Field of the Invention

This invention relates generally to the authentication of users of secure systems and, more particularly, the invention relates to a system through which user tokens required for user authentication are supplied through personal communication devices such as mobile telephones and pages.

Description of the Related Art

Secure systems have traditionally utilized a user ID and password pair to identify and authenticate system users. Operating systems that control local area networks of workstations within a business or institution such as Novell NetWare, Microsoft NT, Windows 2000, and UNIX/Linux typically require submission of a user ID and password combination before allowing access to a workstation.

The incorporation of remote connectivity to secure systems over the Internet has weakened traditional controls imposed by a user's required physical presence within a company's premises and has exposed systems to additional security threats. External users accessing by dial-in or over the Internet, complicated by frequent personnel turnover, require frequent changes in password lists.

Passwords created by users are often combinations of words and names, which are easy to remember but also easily guessed. Guessing passwords is a frequent technique used by "hackers" to break into systems. Therefore, many systems impose regulations on password formats that require mixtures of letters of different cases and symbols and that no part of a password be a word in the dictionary. A user's inability to remember complex combinations of letters, numbers, and symbols often results in the password being written down, sometimes on a note stuck to the side of a workstation.

Present systems face several problems: users dread frequent password changes, frequent password changes with hard-to-remember passwords inevitably result in users

surreptitiously writing down passwords, and security is compromised when users write down their passwords.

The SecurID product, which is distributed by RSA Security Inc., solves many of the aforementioned problems by requiring a two-factor authentication process. The first factor is a user passcode or personal identification number. The second factor is a SecurID card that is possessed by the user. The SecurID card generates and displays unpredictable, one-time-only access codes that automatically change every 60 seconds. The user supplies the displayed code upon logging into a system. The system has a corresponding code generator that allows verification of possession of the card.

The SecurID product, however, requires users to carry an additional item on their person in order to access a secure system. It 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 a mobile phone or a pager.

Attorney Docket No. 50277-0410

Summary of the Invention

A preferred embodiment of the present invention is a password setting system for setting user passwords for a secure system, such as a computer system or a secure area of a building. The password setting system preferably includes a user token server and a communication module. The user token server generates a random token in response to a request for a new password from a user. The server creates a new password by concatenating a secret passcode that is known to the user with the token. The server sets the password associated with the user's user ID to be the new password. The communication module transmits the token to a personal communication device, such as a mobile phone or a pager carried by the user. The user concatenates the secret passcode with the received token in order to form a valid password, which the user submits to gain access to the secure system. Accordingly, 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.

One aspect of the invention is a method for setting passwords. The method includes associating a user ID with a phone number of a personal communication

device. The method also includes generating a new password based at least upon a token. The method also includes setting a password associated with the user ID to be the new password. The method also includes transmitting the token to the personal communication device using the phone number associated with the user ID. In another aspect, the method also includes associating the user ID with a passcode. In another aspect, the new password is generated based additionally upon the passcode. In another aspect, the method also includes receiving a request for the user token. In another aspect, the personal communication device is a mobile phone. In another aspect, the personal communication device is a pager.

An additional aspect of the invention is a password setting system. The system includes a first user database configured to associate a user ID with a phone number of a personal communication device. The system also includes a control module configured to create a password based at least upon a token. The control module is further configured to cause a second user database to associate the password with the user ID. The system also includes a communication module interface configured to cause a communication module to transmit the token to the personal communication device using the phone number associated with the user ID. In another aspect, the first user database and the second user database are the same database. In another aspect, the first user database is further configured to associate the user ID with a passcode, and the control module is further configured to create the password based additionally upon the passcode.

An additional aspect of the invention is a method of regulating access to a secure system. The method includes transmitting a user token to a personal communication device. The method also includes receiving login data in response to a request for authentication information, wherein the login data is based at least upon the user token. The method also includes granting access to the secure system based upon the received login data. In another aspect, the login data is additionally based upon a user ID. In another aspect, the login data comprises a user ID. In another aspect, the login data is additionally based upon a passcode. In another aspect, the login data comprises a user ID and a password. In another aspect, the password comprises a passcode and the token. In another aspect, the password is a concatenation of the passcode and the token.

In another aspect, the password is a hashed concatenation of the passcode and the token. In another aspect the method also includes generating the user token. In another aspect the method also includes receiving a request for the user token. In another aspect, the personal communication device is a mobile phone. In another aspect, the personal communication device is a pager.

An additional aspect of the invention is an access control system. The system includes a user token server configured to transmit a token to a personal communication device. The user token server is further configured to generate a valid password based at least upon the token. The system also includes an authentication module configured to receive at least a submitted password in response to a request for authentication of a user. The authentication module is further configured to grant access to the user if at least the submitted password is based at least upon the token and matches the valid password. In another aspect, the user token server is further configured to generate the valid password based additionally upon a valid passcode that is known to the user. In another aspect, the user token server is further configured to transmit the token in response to a request by the user. In another aspect, the user token server is further configured to associate the valid password with a valid user ID, the authentication module is further configured to receive a submitted user ID in response to the request for authentication, and the authentication module is further configured to grant access to the user if, in addition, the submitted user ID matches the valid user ID.

Brief Description of the Drawings

The present invention will be described below in connection with the attached drawings in which:

Figure 1 illustrates an overview, including system components, of a user authentication system according to a preferred embodiment of the present invention;

Figures 2A-D illustrate login screens that can be used in conjunction with various embodiments of the invention;

Figure 3 illustrates a preferred process performed by the system to authenticate users;

Figure 4 illustrates a preferred embodiment of a user token server;

Figure 5 illustrates a preferred process by which the user token server provides tokens and administrates user accounts;

Figures 6A-C illustrate three embodiments of a token delivery communication link;

Figures 7A-B illustrate two embodiments of a token request communication link; and

Figure 8 illustrates an embodiment of a combined token request and delivery communication link.

Detailed Description of the Embodiments

In the following description, reference is made to the accompanying drawings, which form a part hereof, and which show, by way of illustration, specific embodiments or processes in which the invention may be practiced. Where possible, the same reference numbers are used throughout the drawings to refer to the same or like components. In some instances, numerous specific details are set forth in order to provide a thorough understanding of the present invention. The present invention, however, may be practiced without the specific details or with certain alternative equivalent devices and methods to those described herein. In other instances, well-known methods and devices have not been described in detail so as not to unnecessarily obscure aspects of the present invention.

I. Overview and System Components

Figure 1 illustrates an overview, including system components, of a user authentication system 100 according to a preferred embodiment of the present invention. Figure 2A illustrates login screen that can be used in accordance with the preferred embodiment. Figures 2B-D illustrate a login screens that can be used in accordance with alternative embodiments.

The user authentication system 100 includes an authentication server 102, a text messaging service provider 104, a personal communication device 106 carried by a user 108, and a secure system 110 to which the authentication system 100 regulates access. The personal communication device 106 is preferably a pager or a mobile phone having SMS (short message service) receive capability. SMS is a secure text messaging

capability that is incorporated into most digital mobile phones. The secure system 110 is preferably a Windows NT computer workstation, but may be any system, device, account, or area to which it is desired to limit access to authenticated users. The secure system 110 may be, for example, a user account on a network of computer workstations, a user account on a web site, or a secure area of a building. The secure system 110 is preferably connected to the user authentication server 102 by a computer network 103. In one embodiment, the user authentication server 102 is integrated into the secure system 110.

The user authentication server 102 preferably includes a program or a suite of programs running on a computer system to perform user authentication services. The user authentication server 102 may also include the computer system and hardware upon which the programs run. The user authentication server 102 is preferably configured to require that the user 108 supply authentication information through the secure system 110 in order to gain access to the secure system 110.

The authentication information preferably includes a user ID 152, a passcode 154 and a user token 156. The user 108 preferably commits to memory the user ID 152 and passcode 154. The user ID 152 may be publicly known and used to identify the user 108. The passcode 154 is preferably secret and only known to the user 108. The token 156 is preferably provided only to the user 108 by the user authentication server 102 through the user's personal communication device 106 on an as needed basis. The token 156 preferably has a limited lifespan, such as 1 minute or 1 day. Accordingly, the user 108 needs to be in possession of his personal communication device 106 in order to gain access to the secure system 110. Therefore, if the user's user ID 152 and passcode 154 are compromised, a malicious party still cannot access the secure system without possession of the personal communication device 106.

In the preferred embodiment, the user 108 combines the token 156 with the passcode 154 to form a password 158. For example, the user 108 can combine a valid, memorized passcode of "abcd" with a valid token of "1234" to form a valid password of "abcd1234." In this manner, a login screen such as is illustrated in Figure 2A, which is similar or identical to standard login screens that require a user ID 152 and a password 158, can be used. In an alternative embodiment, the passcode 154 and the token 156 are

submitted separately, as is illustrated in Figure 2B. In another embodiment, the passcode 154 is null in which case the token 156 alone is used as the password 158. In still another embodiment, the token 156 can be requested through the secure system 110 as is illustrated in Figures 2C-D.

The user authentication server 102 is preferably a secure system itself and may be a part or component of the secure system 110. The user authentication server 102 preferably includes an authentication module 112 and a user database 114. The authentication module 112 is preferably identical to the code or software provided with operating systems such as Windows NT that authenticates users upon login. In alternative embodiments, the authentication module 112 may be any code, device, or module capable of 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. The authentication module 112 preferably responds to an authentication request transmitted over the computer network 103 by supplying an authentication confirmation 162 over the network 103. If the user 108 has been authenticated, the confirmation 162 instructs the secure system 110 to allow access to the user 108. The user database 114 is preferably similar or identical to the database accessed by the authentication module 112 that stores user ID and password data (or passcode and token data) in operating systems such as Windows NT. In alternative embodiments, the user database 114 can be any database capable of storing user ID and password data.

The user authentication server 102 preferably also includes a user token server 116 that responds to requests for tokens 160 by generating a token 156 and transmitting the token 156 to the user's personal communication device 106. The user authentication server 102 preferably also resets passwords in the user database 114 based upon generated tokens and passcode data. The user authentication server 102 preferably transmits the tokens 156 over a token delivery communication link 105 to the user's personal communication device 106.

The user authentication server 102 preferably also includes a communication module 118, which is also part of the token delivery communication link 105. The communication module 118 forwards tokens 156 to a text messaging service provider 104, which may be a pager or mobile phone service provider. The text messaging

service provider 104 then forwards the token 156 preferably in the form of a secure text message to the personal communication device 106.

In the preferred embodiment, the communication module 118 is a mobile phone with SMS text messaging send capability. One applicable mobile phone is the presently available Ericsson T-28. The mobile phone 118 is preferably connected to the user authentication server 102 via a presently available serial port cable that makes the phone accessible in a manner similar to a computer modem. Accordingly, the user authentication server 102 can send tokens 156 via the server's mobile phone 118 to the user's mobile phone 106 using SMS. In this case, the server's mobile phone 118 transmits a message including the token 156 to the user's personal communication device 106 using the phone number of the user's personal communication device 106. During the transmission, the message is relayed by the mobile phone service provider 104 to its final destination.

Preferably, the communication module 118 is also configured to receive requests for tokens 160. The user preferably transmits a request for tokens 160 over a request communication link 107. The request communication link 107 may be the same communication link as the delivery communication link 105 or it may be a different link. Various embodiments of the token delivery communication link 105 and the token request communication link 107 will be discussed in Section III below.

In the preferred embodiment, the communication module 118 is a mobile phone that also has SMS text messaging receive capability. The communication module 118 receives an SMS message from the user's mobile SMS send enabled mobile phone 106, and the token server 116 preferably processes the message as a token request 160. The incoming SMS message is tagged with the sending phone's phone number, which the user token server 116 can use to identify the requesting user and respond with a new token 156. The token request 160 may also be in the form of a phone call, in which case the user token server 116 may use a caller ID feature to identify the calling phone number as a valid user's personal communication device 106. The user token server 116 can then respond with a new token 156. Alternatively, the user token server 116 may allow a calling user 108 to enter the phone number of his personal communication device 106 using the mobile phone keypad once a connection has been established.

In an alternative embodiment, the communication module 118 is an ISDN card that is connected to the text messaging service provider 104 preferably via an X.25 connection. The ISDN card 118 preferably transmits new tokens directly to the text messaging service provider 104 for forwarding to the user's personal communication device 106. The ISDN card 118 may also be configured to be accessible at a phone number to receive calls for requests for tokens 160.

Figure 3 illustrates a preferred process 300 performed by the system 100 to authenticate users. At a step 302, the user 108 requests a token from the user token server 116 through the token request communication link 107. In the preferred embodiment, the user's mobile phone 106 has SMS send capability and the user sends an SMS message to the communication module 118 requesting a new token 156. The SMS message need not contain any data in its body since the phone number of the sending mobile phone is automatically sent along with the message. The user token server 116 preferably identifies the user's mobile phone 106 based upon the phone number with which the SMS message is tagged. In an alternative embodiment, the user 108 makes a phone call with his personal communication device 106 to the communication module 118. The user token server 116 identifies the user's personal communication device 106 preferably based upon a caller ID feature. Alternatively, the user 108 may call from any phone and enter in the phone number of his personal communication device 106. As another alternative, the user 108 may request the token 156 through the secure system 110 itself as illustrated in Figures 2C-D. As another alternative, the step 302 may be omitted altogether. In this case, the user token server 116 can automatically send tokens 156 to the user 108 at predetermined intervals, such as once per day where the tokens have a lifespan of one day.

At a step 304 the user token server 116 generates a token 156. The token 156 may be generated by any of a number of methods that preferably produces a random or pseudo-random sequence of numbers and/or digits. The token 156 is preferably long enough such that it cannot be guessed, but short enough such that it is relatively easy to enter, such as six to eight characters.

At a step 306, the token server 116 generates a new password 158. The token server 116 preferably creates the new password 158 by combining the user's passcode

154, which is stored by the user token server 116, with the newly generated token 156. At a step 308, the token server updates the user database 114 with the new password 158. In the case that the user's account in the user database 114 is inactive or deactivated, the token server 116 activates the user's account.

In the preferred embodiment, the token server creates a hash of the password 158 and stores the hash of the password 158 in the user database 114 rather than storing the password 158 itself. The hash is typically performed using a one-way hashing algorithm where the same password always produces the same hash, but where the password cannot be determined from the hash. In typical systems, passwords 158 are stored as hashes rather than as plain text in order to prevent system administrators and others from being able to determine users' passwords by examining the user database 114. Also, when a user 108 submits a password 158 upon login to a secure system 110, the submitted password 158 is immediately hashed using the same one-way hashing algorithm before transmission to the authentication module 112. The authentication module 112 then compares hashes of passwords rather than the passwords themselves to authenticate the user 108. In this manner, passwords 158 need not be transmitted over any communication links or computer networks as clear text. It will be apparent to one skilled in the art that the present invention can be implemented with or without the hashing of passwords and that incorporating hashing of passwords does not substantively affect the scope or spirit of the invention. So as not to unnecessarily obscure aspects of the present invention, a password as referred to herein may be an unhashed or a hashed password. For example, a receipt of a password may be a receipt of an unhashed or hashed password, and a comparison of passwords may be a comparison of unhashed or hashed passwords.

At a step 310, the token server 116 transmits the token 156 to the user's personal communication device 106 via the token delivery communication link 105. In the preferred embodiment, the communication module 118 is a mobile phone, and the user token server 116 uses the SMS send capability of the phone 118 to send an SMS message including the token 156 to the user's personal communication module 106. At a step 312, the user 108 receives the token through his personal communication device 106.

At a step 314, the user 108 logs into the secure system 110 using the user ID 152 and the password 158. In the preferred embodiment, the user 108 combines the passcode 154 and the token 156 by concatenation to form the password 158. In an alternative embodiment, the passcode 154 and the token 156 are submitted separately.

At a step 316, the secure system 110 transmits login data 159 to the user authentication server 102 over the computer network 103 for authentication of the user 108. The login data 159 preferably includes the user ID 152 and a hash of the password 158 that the secure system 110 creates in order to avoid sending the password 158 over the computer network 103 in clear text. Alternatively, the login data 159 may include a hash of the passcode 154 and the token 156. As another alternative, the password 158, or the passcode 154 and token 156 are not hashed.

At a step 318, the user authentication server 102 authenticates the user 108 based upon the login data 159. In order to authenticate the user 108, 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.

At a step 320, the user authentication server 102 transmits an authentication confirmation 162 to the secure system 110. At a step 322, the secure system 110 allows the user 108 access based upon the authentication confirmation 162.

II. The User Token Server

Figure 4 illustrates a preferred embodiment of the user token server 116. The user token server 116 preferably includes a process or program running on or in conjunction with the user authentication server 102. The user token server 116 may, however, include a computer upon which the process or program executes. The user token server 116 preferably includes a control module 402, a supplemental user database 404, a communication module interface 406, and a token generation module 408. The various modules and components of the user token server 116 are described herein from a functional perspective. The various functional components may, however, be seamlessly integrated into one or more executable programs, data structures, and/or physical components.

The control module 402 preferably serves as the top level component of the user token server 116. The control module 402 preferably handles any tasks or functions not handled by the other modules of the token server 116, in addition to controlling the other modules. The control module 402 preferably maintains a supplemental user database 404, which preferably stores associations of user IDs with passcodes, phone numbers of users' personal communication devices, and any other supplemental user data. The other supplemental user data may include one or more of: whether an account is active, the expiration time of passwords, and the frequency with which tokens may be automatically distributed. The supplemental user database 404 is preferably accessed and modified through an administrator user interface 403 provided by the control module 402. The administrator user interface 403 allows administration of user privileges by adding, modifying and removing user IDs, passcodes, and phone numbers from the supplemental user database 404.

In the preferred embodiment, the supplemental user database 404 is maintained separately from the user database 114 of the user authentication server 102. In this configuration, the user database 114 supplied with an OEM system need not be modified or reconfigured. The user token server 116 can be added to existing secure systems in order to provide additional security functionality. In an alternative embodiment, the supplemental user database 404 may be integrated into the user database 114. In this case, user authentication module 102 is preferably configured and supplied as a single integrated component.

Figure 5 illustrates a preferred process 500 by which the user token server 116 provides tokens 156 and administers user accounts. The process 500 is described below in conjunction with the description of the functionality of the various modules and components of the user token server 116.

At a step 502, the control module 402 associates a user ID with a passcode 154 and a phone number of a user's personal communication device 106. Upon initially setting up an account, the association can be performed manually by a system administrator through the administrator user interface 403. The administrator user interface 403 preferably solicits a desired user ID 152, passcode 154, and phone number from a system administrator. The control module 402 then preferably creates a

deactivated user account with a user ID 152 for the secure system 110 on the user database 114 of the user authentication server 102. The control module 402 preferably accesses the user database 114 using an application program interface (API) (not illustrated), which is typically provided with OEM systems. The control module 402 also preferably creates an entry in the supplemental user database 404 including the user ID 152, the passcode 154, and the phone number.

At a step 504, the user token server 116 receives a token request 160 from the user 108, possibly in order to activate his deactivated account. The token request 160 is preferably received through the communication module 118, which the control module 402 preferably controls through a communication module interface 406. The communication module interface 406 is preferably a device driver tailored for the specific implementation of the communication module 118. In alternative embodiments, the user may request the token 156 through the secure system 110 itself, as illustrated in Figures 2C-D. In this case, the request 160 may be received through the computer network 103.

At a step 506, the control module 402 associates the token request 160 with a valid user ID 152. The control module 402 may make this association based upon a supplied phone number by querying the supplemental user database 404. In one embodiment, if the user ID 152 is supplied in conjunction with the request 160, the step 506 is not performed .

At a step 508, the token generation module 408 generates a token by a method that produces a random or pseudo-random sequence of numbers or digits or both numbers and digits. Many methods are presently known for producing such random sequences. The token generation module 408 preferably passes the newly generated token 156 to the control module 402.

At a step 510, the control module 402 generates a new password 158 based upon the generated token 156 and the passcode 154 associated with the user ID 152 as listed in the supplemental user database 404. The new password 158 is preferably generated by concatenating the passcode 154 and the token 156.

At a step 512, the control module 402 sets or resets the password associated with the user ID 152 in the user database 114. In the preferred embodiment, the control

module 402 sets the password to be a one-way hash of the newly generated password 158. In alternative embodiments, the password 158 need not be hashed. In the case the user's account has been deactivated, the control module 402 activates the user ID 152 in the user database 114. The control module 402 preferably accesses the user database 114 through the database API (not illustrated).

At a step 514, the control module 402 transmits the token 156 to the user's personal communication device 106 preferably based upon the phone number associated with the user ID 152 in the supplemental user database 404. In the preferred embodiment, the control module 402 causes the communication module 118 to generate and send an SMS message containing the token 156 to the user's mobile phone. In an alternative embodiment, the communication module 118 may call the phone number of the user's pager and transmit the token 156 as the page data.

At a step 516, the user 108 is able to access the secure system 110 by logging in using the supplied token 156. The user 108 preferably concatenates his memorized secret passcode 154 with the valid token 156 to create the password 158. The user then logs in using his user ID 152 and the password 158.

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.

Finally, the process 500 repetitively continues either from the step 502, if a new user 108 is to be added, or from the step 504 if an existing user 108 requests a token 156.

III. Token Delivery and Request Communication Links

Figures 6A-C illustrate three embodiments of the token delivery communication link 105. Figures 7A-B illustrate two embodiments of the token request communication link 107. In some embodiments, the same communication link may be used as the token delivery communication link 105 and the token request communication link 107. Figure 8 illustrates an embodiment of a combined token request and delivery communication link that can function in conjunction with a mobile phone without text messaging capability. Additionally, communication technologies other than those

illustrated here by example may be used to implement the communication links 105 and 107.

Figure 6A illustrates a preferred embodiment of the token delivery communication link 105. The communication module 118 is a mobile phone 602 with SMS send capability. The mobile phone 602 sends an SMS message 603 including the token 156 to the user's mobile phone 604. While in transit, the message 603 is received and retransmitted by the SMS system 606 of a mobile phone service provider.

Figure 6B illustrates a first alternative embodiment of the token delivery communication link 105. In this case, the communication module 118 is an ISDN card or an X.25 connection card 612 that connects to an SMS gateway 616 of a mobile phone service provider via an ISDN or X.25 connection 613. The card 612 transmits the token 156 to the SMS gateway 616, which then creates an SMS message 615 and transmits the message 615 to the user's mobile phone 614.

Figure 6C illustrates a second alternative embodiment of the token delivery communication link 105. 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. The paging service provider 626 answers and the phone dialer 622 enters a numeric token 156 to be transmitted to the pager 624. The paging service provider 626, in turn, sends a page 625 containing the token 156 to the user's pager 624.

Figure 7A illustrates a preferred embodiment of the token request communication link 107. The personal communication device 106 is preferably the mobile phone 604, the communication module 118 is preferably the mobile phone 602, and the text messaging service provider 104 is preferably the SMS system 606 of the preferred embodiment of the token delivery communication link 105 (Figure 6A). Alternatively, the communication module 118 may be the ISDN card or X.25 connection card 612 connected through the ISDN or X.25 connection 613 as in the first alternative embodiment of the token delivery communication link 105 (Figure 6B). The mobile phone 604 preferably sends an SMS message 703 as a token request 160 to the mobile phone 602 or the ISDN card 612. The SMS message 703 may have a blank

message body but the message preferably includes the sending phone's phone number in a tag or header field. While in transit, the message 603 is received and retransmitted by the SMS system 606. The user token server 116 preferably identifies the sending phone's phone number, and if the phone number matches a valid user ID 152, the token server 116 processes the message 703 as a token request 160.

Figure 7B illustrates a first alternative embodiment of the token request communication link 107 in accordance with the token request and login screens of Figures 2C-D. The user 108 makes the token request 160 through a first login screen (Figure 2C) on the secure system 110. The token request 160 in this case preferably includes the user's user ID 152 and is preferably transmitted through the computer network 103 to the user token server 116 through a network interface card 702. In this case, the token request 160 need not be communicated through the communication module 118. Also, the personal communication device 106 need not be used in requesting the token 156 but is preferably used in delivering the token 156.

Figure 8 illustrates a combined token request and delivery link in which the personal communication device 106 is preferably a mobile phone. The communication module 118 is preferably an automated telephone response system 802 with a caller ID capability. The user 108 places a phone call 803 to the telephone response system 802, which identifies the calling phone 804 using caller ID. The telephone response system 802 interprets the call as a token request 160 and responds by generating a voice synthesized recitation of the token 156 that the user hears through the mobile phone 804. The mobile phone 804, in this case, need not have any text messaging or SMS capability.

In still other embodiments, various other technologies and combinations of technologies, which will be apparent to one skilled in the art, can be used to implement the token delivery 105 and token request 107 communication links. For example, a token request may be made through a land line phone, and in response, a token may be delivered to a mobile phone.

IV. Conclusion

Although the invention has been described in terms of certain preferred embodiments, other embodiments that are apparent to those of ordinary skill in the art,

including embodiments which do not provide all of the features and advantages set forth herein, are also within the scope of this invention. Accordingly, the scope of the invention is defined by the claims that follow. In the claims, a portion shall include greater than none and up to the whole of a thing; encryption of a thing shall include encryption of a portion of the thing; a password may be an unhashed or a hashed password. In the method claims, reference characters are used for convenience of description only, and do not indicate a particular order for performing the method.

0756855.0 - 5256715.00

WHAT IS CLAIMED IS:

1. A method for setting passwords comprising:

(A) associating a user ID with a phone number of a personal communication device;

(B) generating a new password based at least upon a token;

(C) setting a password associated with the user ID to be the new password; and

(D) transmitting the token to the personal communication device using the phone number associated with the user ID.

2. The method of Claim 1, further comprising

(E) associating the user ID with a passcode.

3. The method of Claim 2, wherein (B) is based additionally upon the passcode.

4. The method of Claim 1, further comprising

(F) receiving a request for the user token.

5. The method of Claim 4, wherein (B), (C), and (D) are performed in response to (F).

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

7. The method of Claim 1, wherein the personal communication device is a pager.

8. A password setting system comprising:

a first user database configured to associate a user ID with a phone number of a personal communication device;

a control module configured to create a password based at least upon a token, the control module further configured to cause a second user database to associate the password with the user ID; and

a communication module interface configured to cause a communication module to transmit the token to the personal communication device using the phone number associated with the user ID.

9. The password setting system of Claim 8, wherein the first user database and the second user database are the same database.

10. The password setting system of Claim 8, wherein the first user database is further configured to associate the user ID with a passcode, and wherein the control module is further configured to create the password based additionally upon the passcode.

11. A method of regulating access to a secure system, the method comprising:

(A) transmitting a user token to a personal communication device;

(B) receiving login data in response to a request for authentication information, wherein the login data is based at least upon the user token; and

(C) granting access to the secure system based upon the received login data.

12. The method of Claim 11, wherein the login data is additionally based upon a user ID.

13. The method of Claim 11, wherein the login data comprises a user ID.

14. The method of Claim 12, wherein the login data is additionally based upon a passcode.

15. The method of Claim 11, wherein the login data comprises a user ID and a password.

16. The method of Claim 15, wherein the password comprises a passcode and the token.

17. The method of Claim 16, wherein the password is a concatenation of the passcode and the token.

18. The method of Claim 16, wherein the password is a hashed concatenation of the passcode and the token.

19. The method of Claim 11, further comprising

(D) generating the user token.

20. The method of Claim 19, further comprising

(E) receiving a request for the user token.

21. The method of Claim 20, wherein (A) and (D) are performed in response to (E).

22. The method of Claim 11, wherein the personal communication device is a mobile phone.

23. The method of Claim 11, wherein the personal communication device is a pager.

24. An access control system comprising:

a user token server configured to transmit a token to a personal communication device, the user token server further configured to generate a valid password based at least upon the token; and

an authentication module configured to receive at least a submitted password in response to a request for authentication of a user, the authentication module further configured to grant access to the user if at least the submitted password is based at least upon the token and matches the valid password.

25. The access control system of Claim 24, wherein the user token server is further configured to generate the valid password based additionally upon a valid passcode that is known to the user.

26. The access control system of Claim 24, wherein the user token server is further configured to transmit the token in response to a request by the user.

27. The access control system of Claim 25, wherein the user token server is further configured to associate the valid password with a valid user ID, wherein the authentication module is further configured to receive a submitted user ID in response to the request for authentication, and wherein the authentication module is further configured to grant access to the user if, in addition, the submitted user ID matches the valid user ID.

USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION

Abstract of the Disclosure

A password setting system for a secure system includes a user token server and a communication module. The user token server generates a random token in response to a request for a new password from a user. The server creates a new password by concatenating a secret passcode that is known to the user with the token. The server sets the password associated with the user's user ID to be the new password. The communication module transmits the token to a personal communication device, such as a mobile phone or a pager carried by the user. The user concatenates the secret passcode with the received token in order to form a valid password, which the user submits to gain access to the secure system. Accordingly, 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.

H:\DOCS\ASF\ASF-1351.DOC
030600

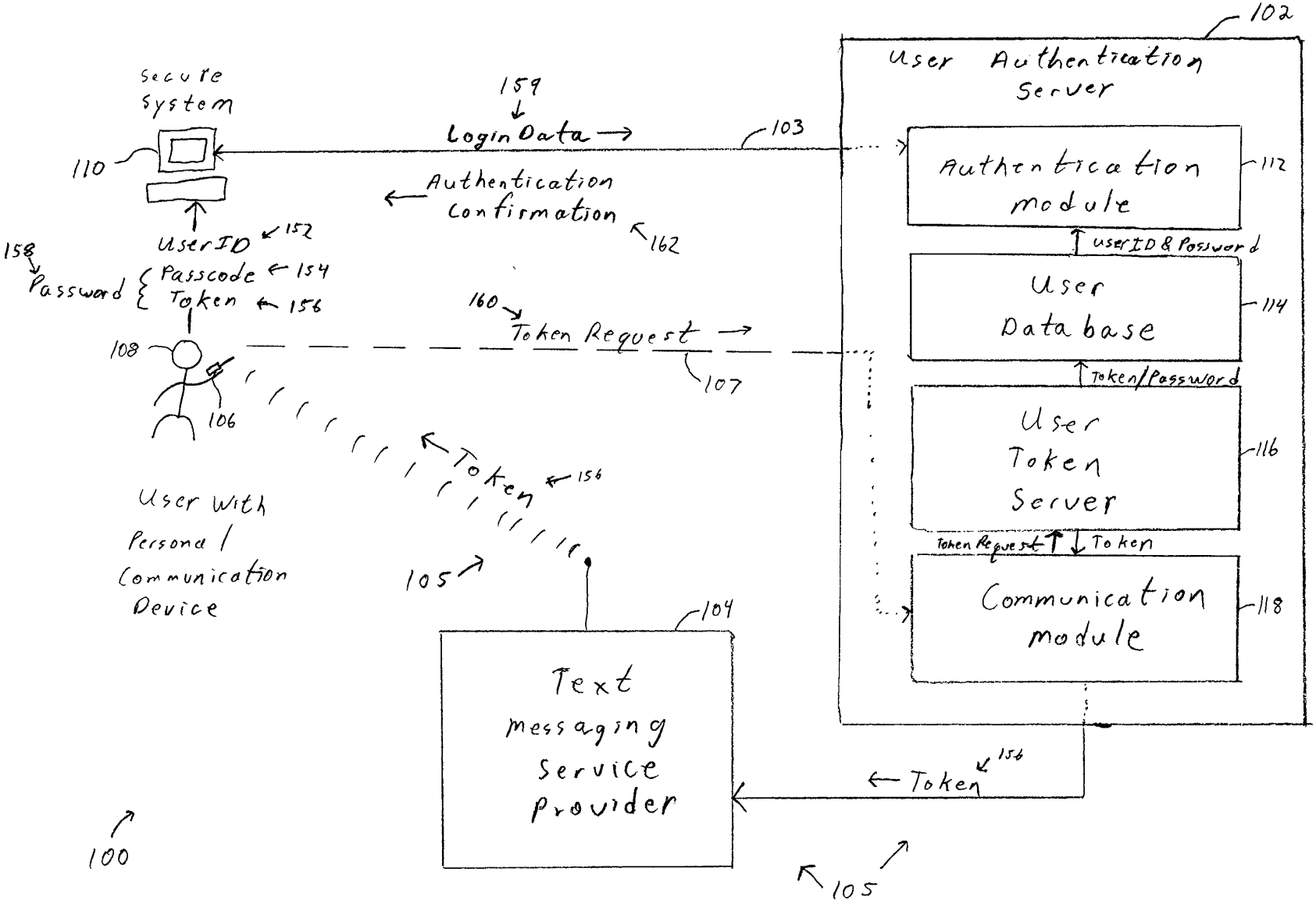

102
User Authentication Server
Secure System
110
159
Login Data
103
Authentication Confirmation
162
Authentication module
112
UserID & Password
User Database
114
158
Password
Passcode
154
Token
156
160
Token Request
107
108
106
Token/Password
User Token Server
116
Token
Token Request
Token
User With Persona / Communication Device
105
Communication module
118
104
Text messaging Service Provider
Token
156
100
105

Fig 1

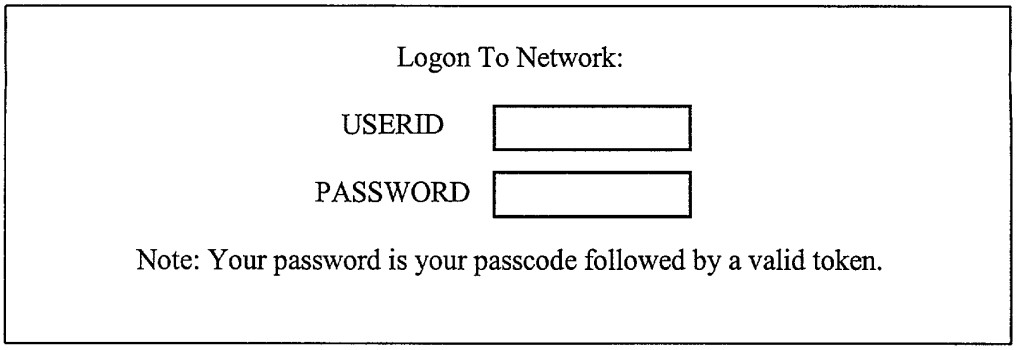


Fig 2A

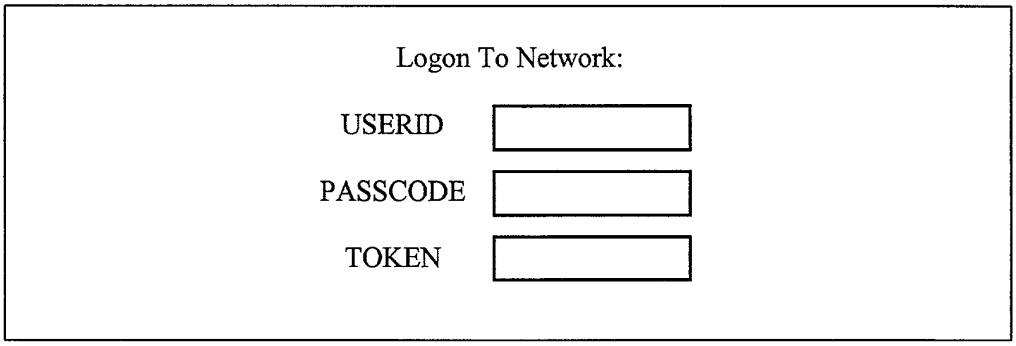


Fig 2B

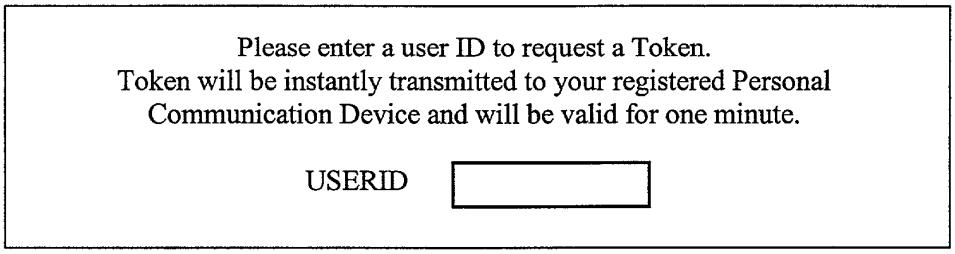


Fig 2C

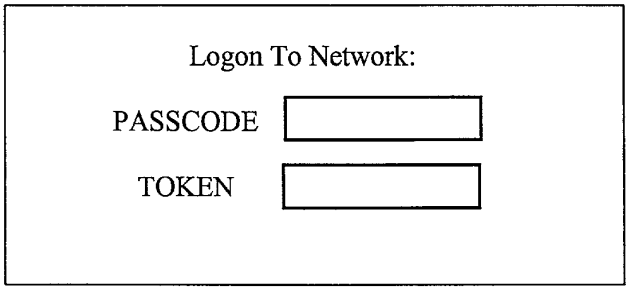


Fig 2D

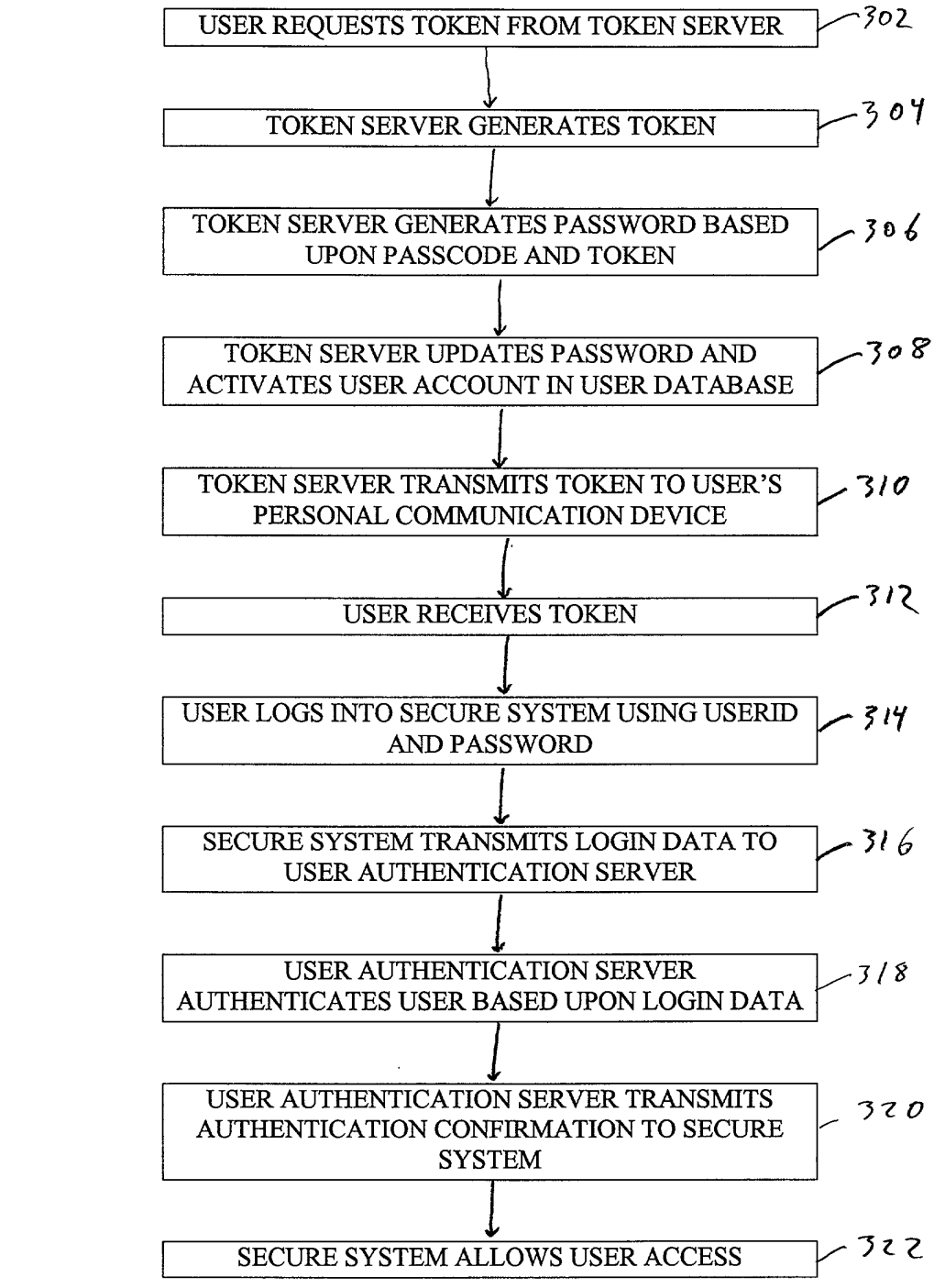

USER REQUESTS TOKEN FROM TOKEN SERVER
302
TOKEN SERVER GENERATES TOKEN
304
TOKEN SERVER GENERATES PASSWORD BASED UPON PASSCODE AND TOKEN
306
TOKEN SERVER UPDATES PASSWORD AND ACTIVATES USER ACCOUNT IN USER DATABASE
308
TOKEN SERVER TRANSMITS TOKEN TO USER'S PERSONAL COMMUNICATION DEVICE
310
USER RECEIVES TOKEN
312
USER LOGS INTO SECURE SYSTEM USING USERID AND PASSWORD
314
SECURE SYSTEM TRANSMITS LOGIN DATA TO USER AUTHENTICATION SERVER
316
USER AUTHENTICATION SERVER AUTHENTICATES USER BASED UPON LOGIN DATA
318
USER AUTHENTICATION SERVER TRANSMITS AUTHENTICATION CONFIRMATION TO SECURE SYSTEM
320
SECURE SYSTEM ALLOWS USER ACCESS
322
300

Fig 3

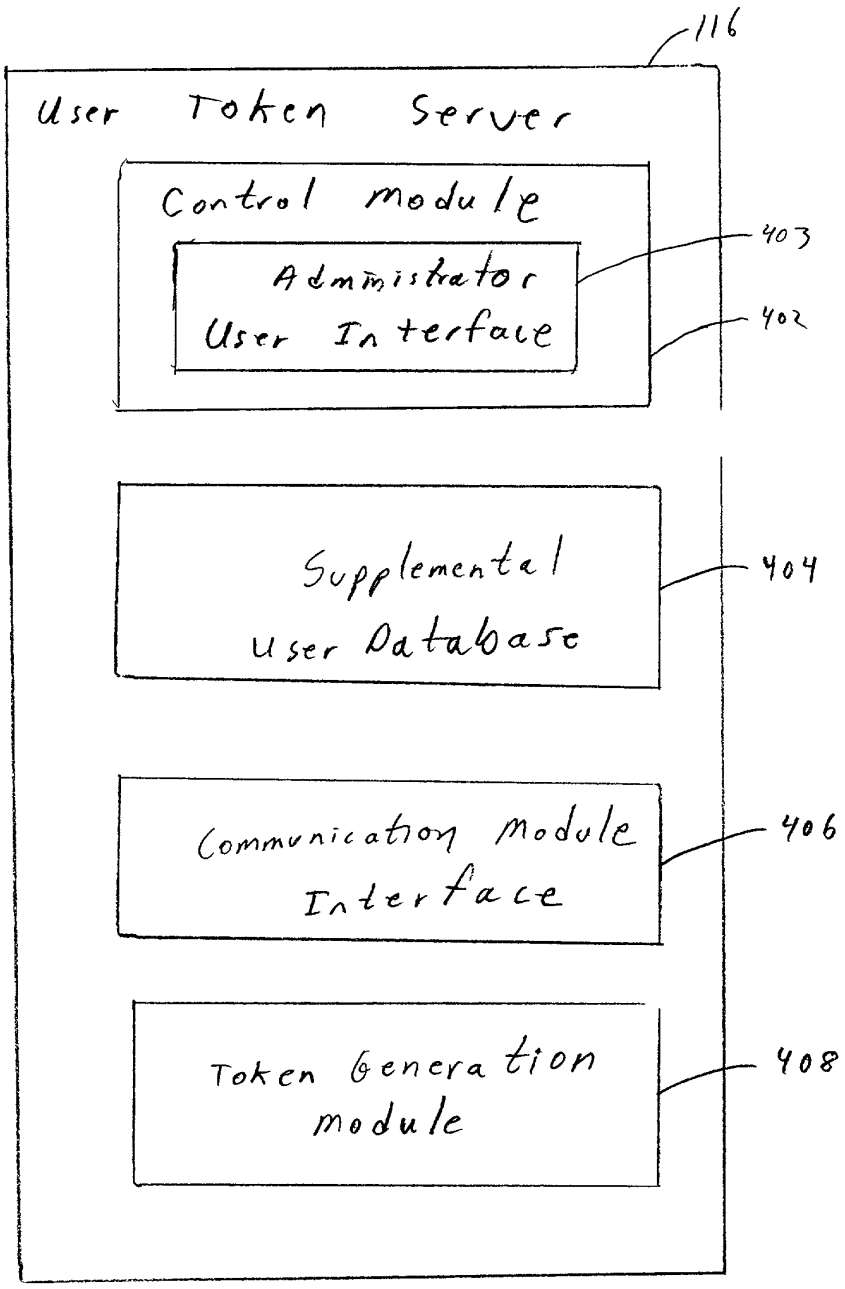
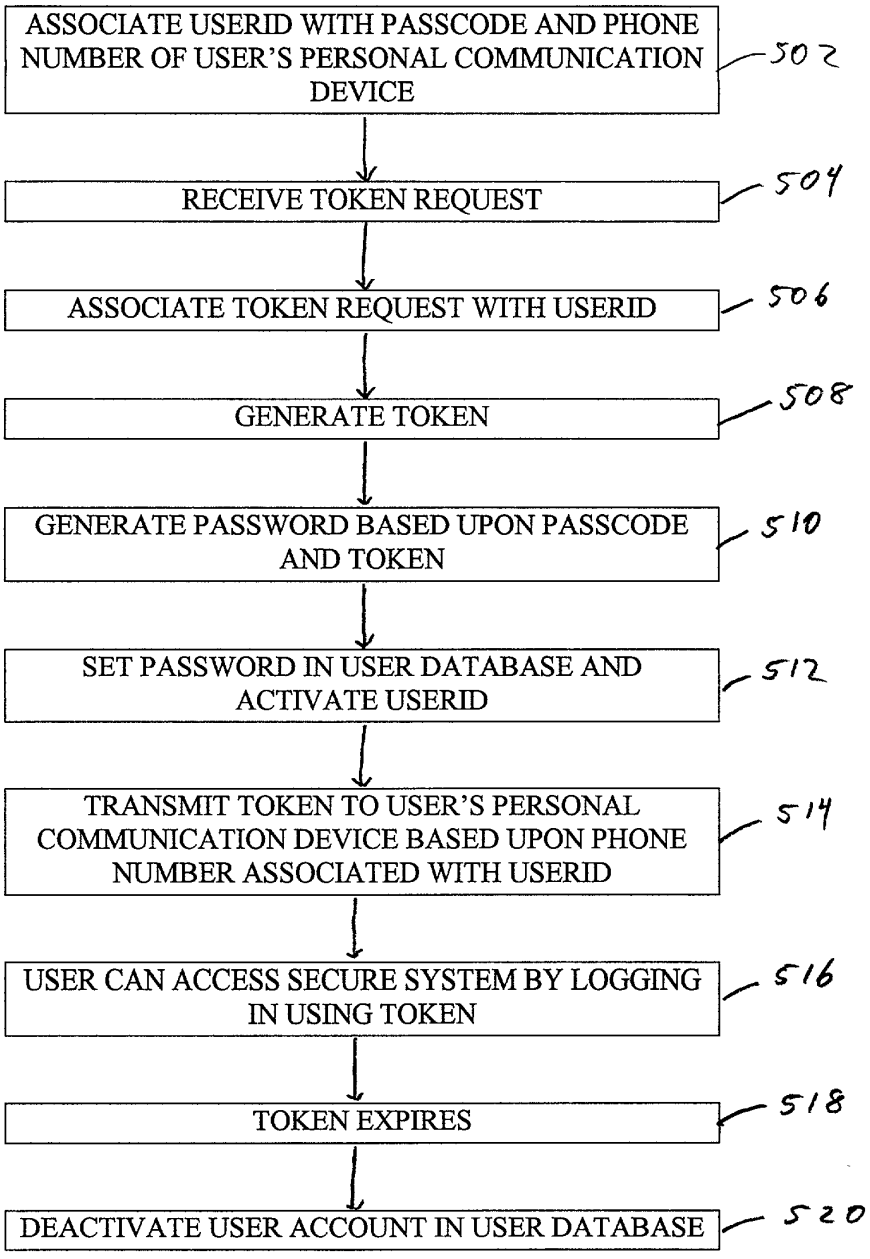

116
User Token Server
Control module
Administrator User Interface
403
402
Supplemental User Database
404
Communication module Interface
406
Token Generation module
408

Fig 4


ASSOCIATE USERID WITH PASSCODE AND PHONE NUMBER OF USER'S PERSONAL COMMUNICATION DEVICE
502
RECEIVE TOKEN REQUEST
504
ASSOCIATE TOKEN REQUEST WITH USERID
506
GENERATE TOKEN
508
GENERATE PASSWORD BASED UPON PASSCODE AND TOKEN
510
SET PASSWORD IN USER DATABASE AND ACTIVATE USERID
512
TRANSMIT TOKEN TO USER'S PERSONAL COMMUNICATION DEVICE BASED UPON PHONE NUMBER ASSOCIATED WITH USERID
514
USER CAN ACCESS SECURE SYSTEM BY LOGGING IN USING TOKEN
516
TOKEN EXPIRES
518
DEACTIVATE USER ACCOUNT IN USER DATABASE
520

500

Fig 5

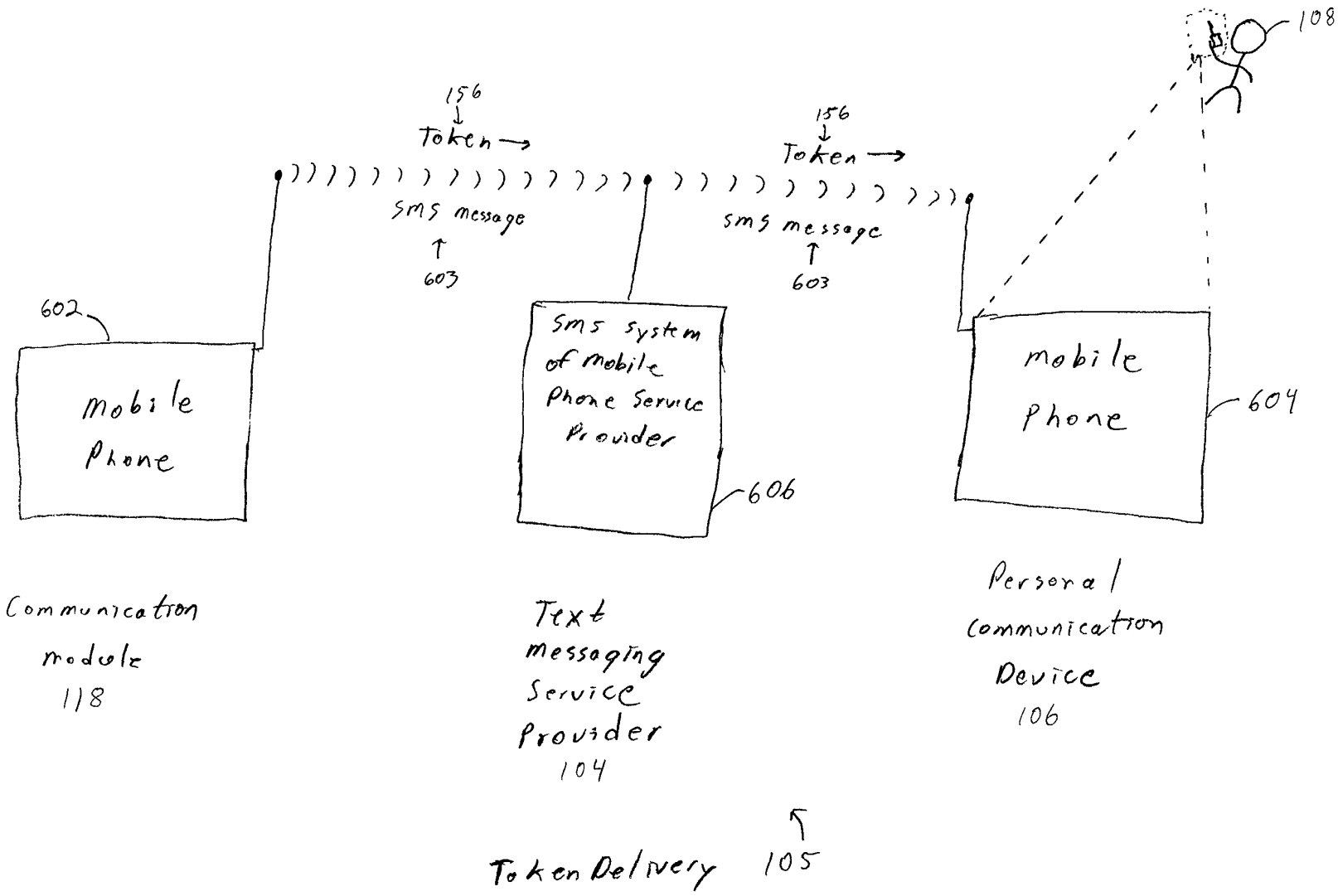

156
Token
156
Token
108
SMS message
603
SMS message
603
602
SMS system of mobile Phone Service Provider
606
mobile Phone
604
mobile Phone
Communication module 118
Text messaging Service Provider 104
Personal communication Device 106
Token Delivery 105

Fig 6A

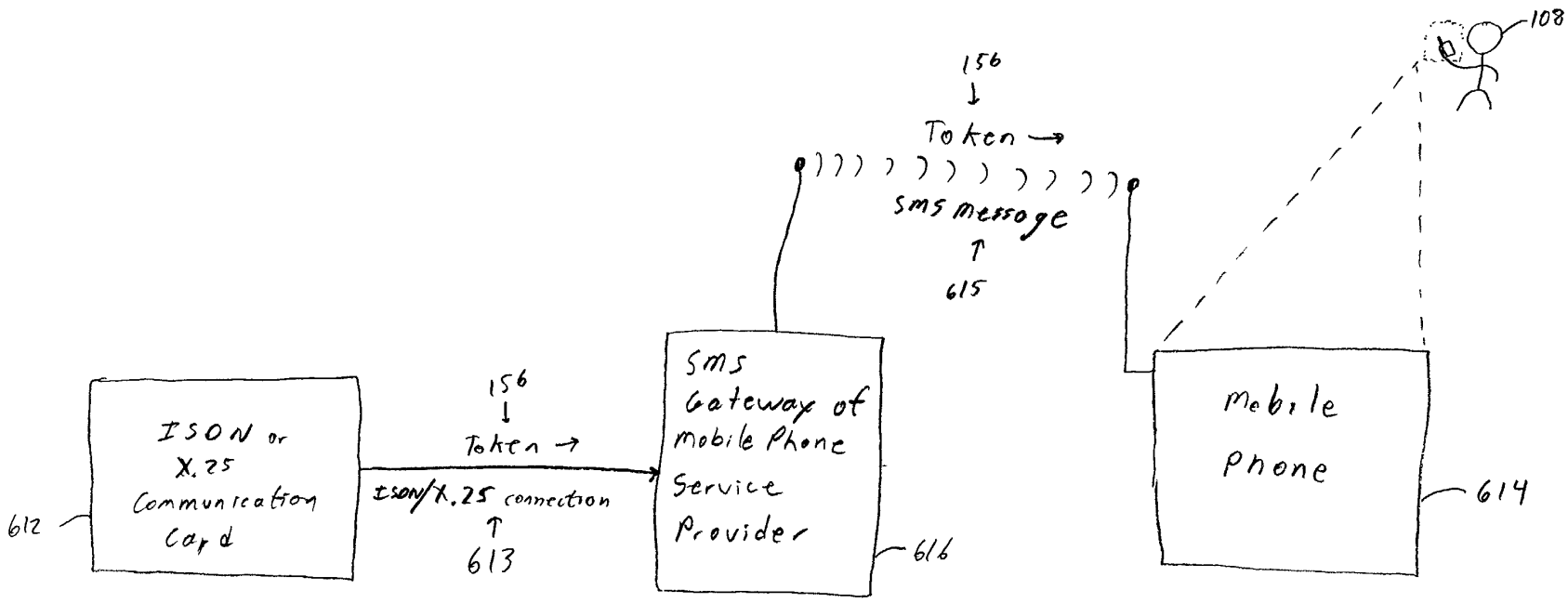

108
156
Token
SMS message
615
SMS Gateway of Mobile Phone Service Provider
616
Mobile Phone
614
156
Token
ISON or X.25 Communication Card
612
ISON/X.25 connection
613
Communication module 118
Text Messaging service Provider 104
Personal Communication Device 106
Token Delivery
105

Fig 6B

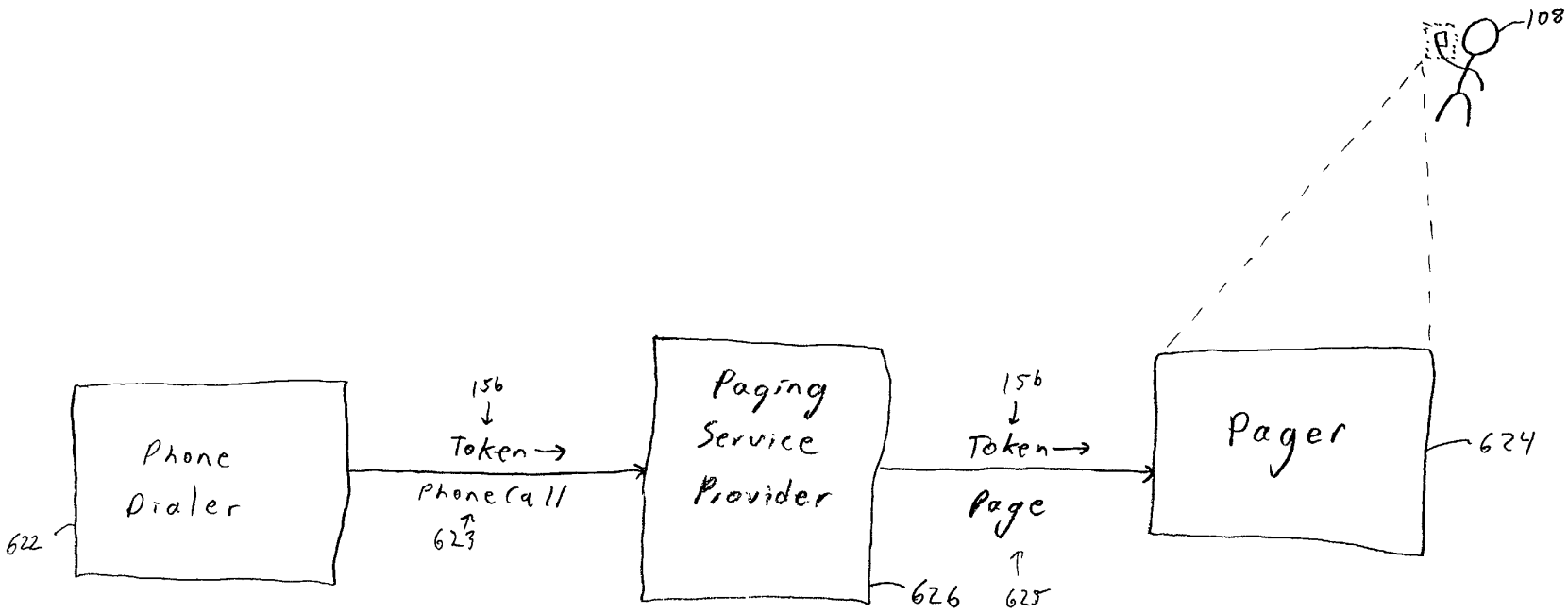

108
Phone Dialer
622
156
Token
Phone Call
623
Paging Service Provider
626
156
Token
Page
625
Pager
624
Communication module 118
Text Messaging Service Provider 104
Personal Communication Device 106
Token Delivery
105

Fig 6C

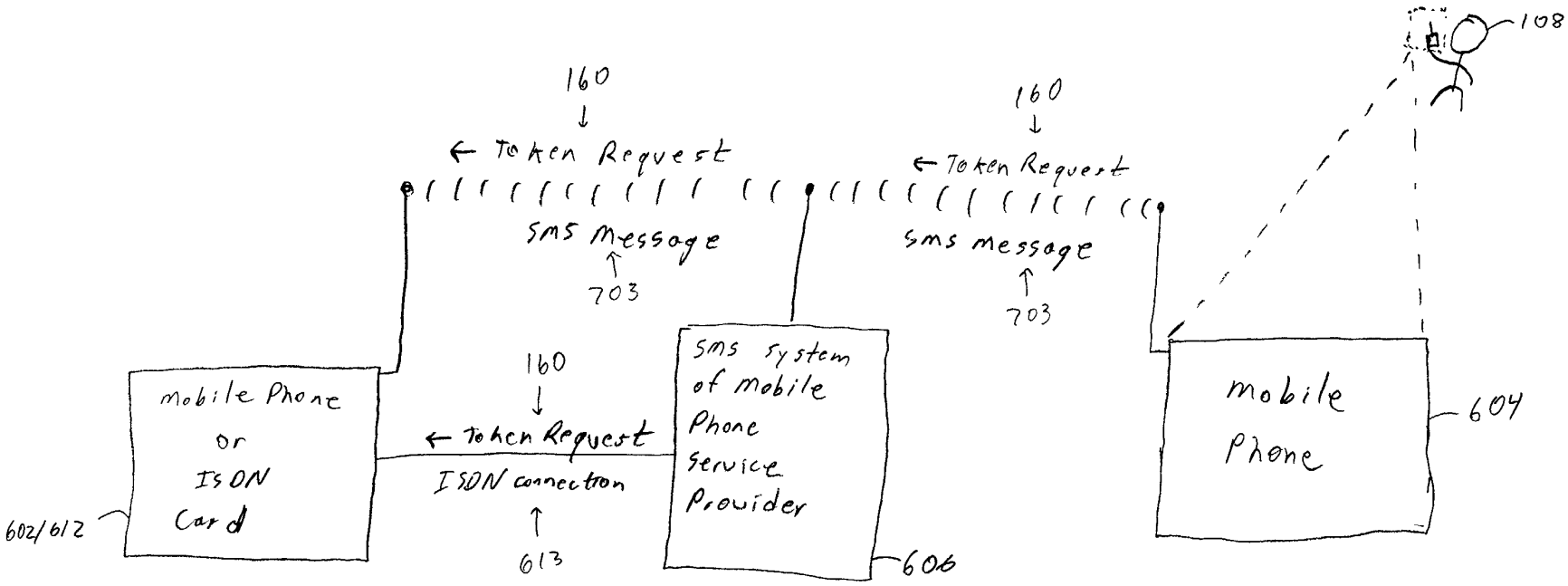
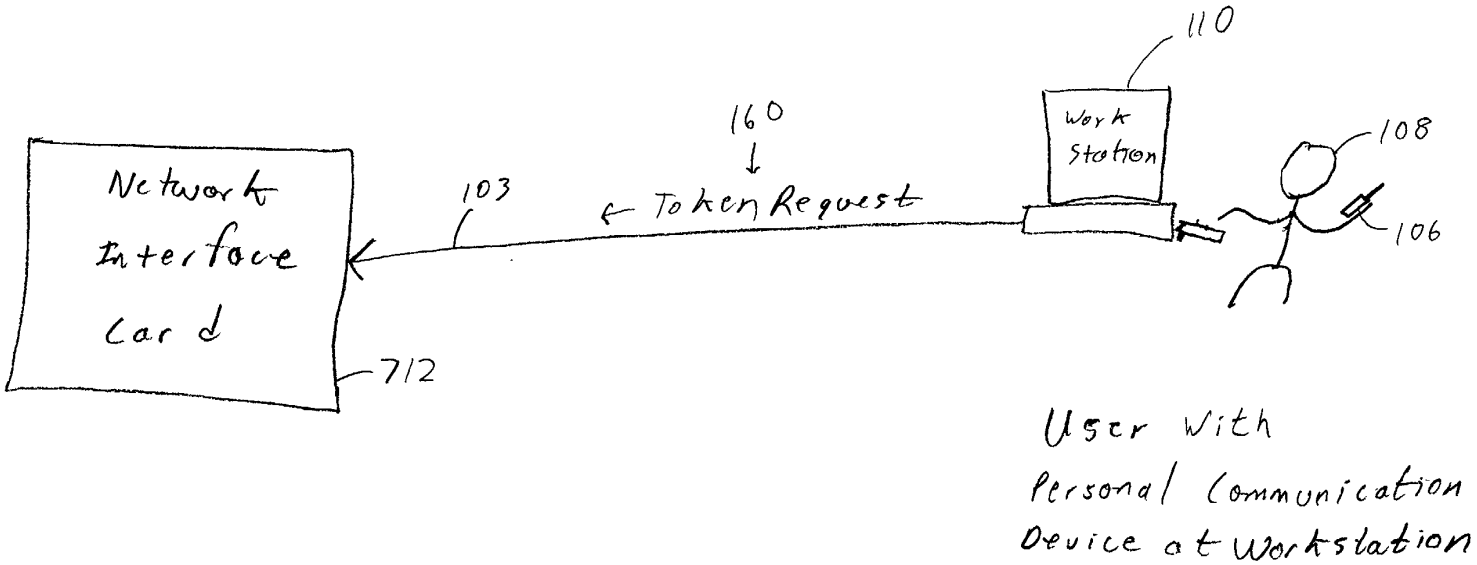
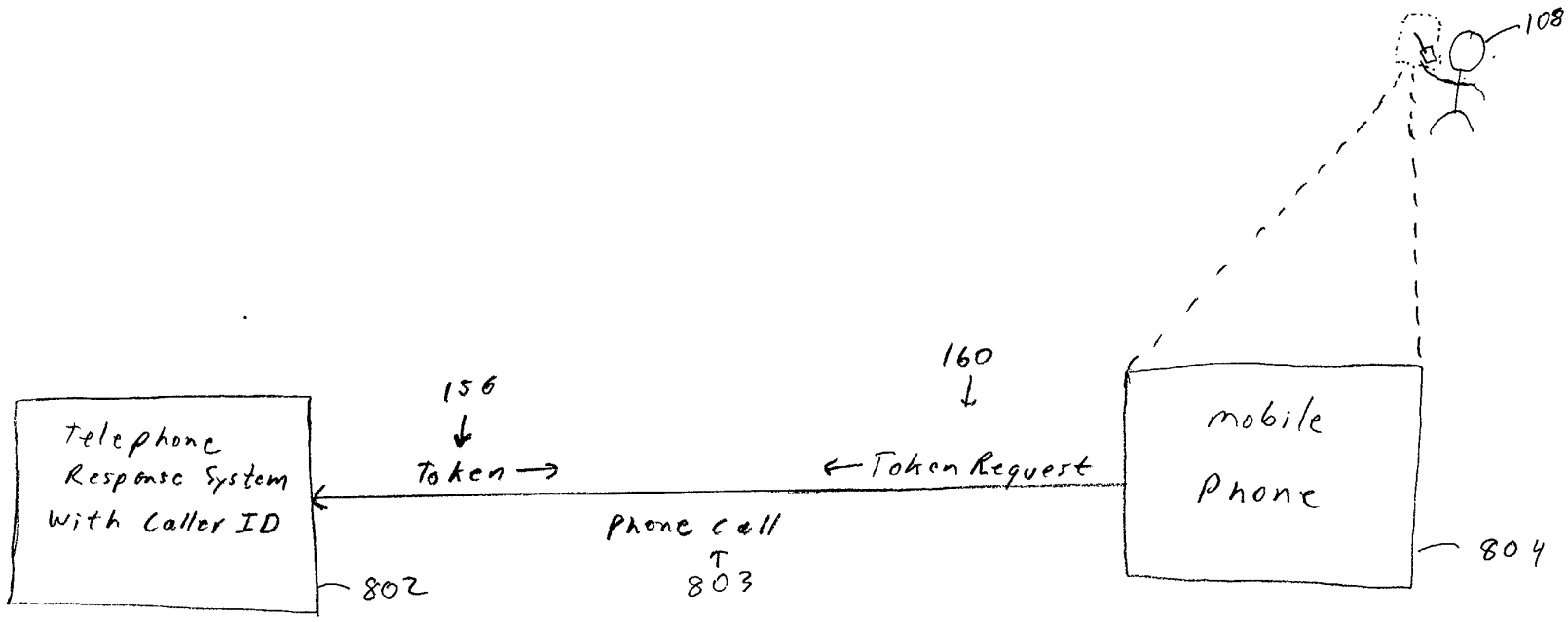

160
Token Request
SMS Message
703
160
Token Request
SMS Message
703
108
160
Token Request
ISON connection
613
Mobile Phone or ISON Card
602/612
SMS System of Mobile Phone Service Provider
606
Mobile Phone
604
Communication Module
118
Text Messaging Service Provider
104
Personal Communication Device
106
Token Request
107

Fig 7A



Token Request 107

Fig 7B



Token Request and Delivery

Fig 8

BEST AVAILABLE COPY

09/519829 U.S. PTO 03/06/00

Subclass | Class | ISSUE CLASSIFICATION

PATENT NUMBER

U.S. UTILITY Patent Application

O.I.P.E.

SCANNED ____ Q.A. ____

PATENT DATE

APPLICATION NO.	CONT/PRIOR	CLASS	SUBCLASS	ART UNIT	EXAMINER
09/519829		713	202	~~2777~~ 2755 2134	~~Hayes~~ Heneghan

APPLICANTS: Sten-Olov Engberg
Ake Jonsson

TITLE: Use personal communication devices for userauthentication

APPLICANT(S)

PTO-2040
12/99

ISSUING CLASSIFICATION

ORIGINAL		CROSS REFERENCE(S)	
CLASS	SUBCLASS	CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)
INTERNATIONAL CLASSIFICATION			
			☐ Continued on Issue Slip Inside File Jacket

☐ TERMINAL DISCLAIMER	DRAWINGS			CLAIMS ALLOWED	
	Sheets Drwg.	Figs. Drwg.	Print Fig.	Total Claims	Print Claim for O.G.
☐ The term of this patent subsequent to _____ (date) has been disclaimed.				NOTICE OF ALLOWANCE MAILED	
☐ The term of this patent shall not extend beyond the expiration date of U.S Patent. No. _____				ISSUE FEE	
				Amount Due	Date Paid
☐ The terminal ____months of this patent have been disclaimed.				ISSUE BATCH NUMBER	

(Assistant Examiner) (Date)

(Primary Examiner) (Date)

(Legal Instruments Examiner) (Date)

WARNING:
The information disclosed herein may be restricted. Unauthorized disclosure may be prohibited by the United States Code Title 35, Sections 122, 181 and 368. Possession outside the U.S. Patent & Trademark Office is restricted to authorized employees and contractors only.

Form PTO-436A
(Rev. 6/99)

FILED WITH: ☒ DISK (CRF) ☐ FICHE ☐ CD-ROM
(Attached in pocket on right inside flap)

(FACE)

BEST AVAILABLE COPY

SEARCHED

Class	Sub.	Date	Exmr.
380 455	247 249 411	12/4/03	MM
713 705 235	202 74 382.5	5/13/04	MM

INTERFERENCE SEARCHED

Class	Sub.	Date	Exmr.

SEARCH NOTES
(INCLUDING SEARCH STRATEGY)

	Date	Exmr.
Searched EAST, EPO, JPO, Derwent keywords: password, cell, mobile, phone, salt, append	12/4/03	MM
EAST, keywords personal communication, mobile, cell, pager, cordless, appeal, account, create, time, password, temporary, guest	5/13/04	MM

(RIGHT OUTSIDE)

ISSUE SLIP STAPLE AREA (for additional cross references)

POSITION	INITIALS	ID NO.	DATE
FEE DETERMINATION	Rmp	12	3/4/08
O.I.P.E. CLASSIFIER			3/20
FORMALITY REVIEW			
RESPONSE FORMALITY REVIEW		5983	4-14-08
		5983	7-24-08

INDEX OF CLAIMS

✔ ..... Rejected
= ..... Allowed
— (Through numeral)... Canceled
÷ ..... Restricted
N ..... Non-elected
I ..... Interference
A ..... Appeal
O ..... Objected

Claim Final	Claim Original	Date									
	1	12/4/2007	5/19/2008								
	2										
	3										
	4										
	5										
	6										
	7										
	8										
	9										
	10										
	11										
	12										
	13										
	14										
	15										
	16										
	17										
	18										
	19										
	20										
	21										
	22										
	23										
	24										
	25										
	26										
	27										
	28	✓	✓								
	29	✓	✓								
	30	✓	✓								
	31	✓	✓								
	32	✓	✓								
	33	✓	✓								
	34	✓	✓								
	35	✓	✓								
	36	✓	✓								
	37	✓	✓								
	38	✓	✓								
	39	✓	✓								
	40	✓	✓								
	41	✓	✓								
	42	✓	✓								
	43	✓	✓								
	44	✓	✓								
	45	✓	✓								
	46	✓	✓								
	47	✓	✓								
	48	✓	✓								
	49	✓	✓								
	50	✓	✓								

Claim Final	Claim Original	Date									
	51	✓	✓								
	52	✓	✓								
	53	✓	✓								
	54										
	55										
	56										
	57										
	58										
	59										
	60										
	61										
	62										
	63										
	64										
	65										
	66										
	67										
	68										
	69										
	70										
	71										
	72										
	73										
	74										
	75										
	76										
	77										
	78										
	79										
	80										
	81										
	82										
	83										
	84										
	85										
	86										
	87										
	88										
	89										
	90										
	91										
	92										
	93										
	94										
	95										
	96										
	97										
	98										
	99										
	100										

Claim Final	Claim Original	Date									
	101										
	102										
	103										
	104										
	105										
	106										
	107										
	108										
	109										
	110										
	111										
	112										
	113										
	114										
	115										
	116										
	117										
	118										
	119										
	120										
	121										
	122										
	123										
	124										
	125										
	126										
	127										
	128										
	129										
	130										
	131										
	132										
	133										
	134										
	135										
	136										
	137										
	138										
	139										
	140										
	141										
	142										
	143										
	144										
	145										
	146										
	147										
	148										
	149										
	150										

If more than 150 claims or 10 actions staple additional sheet here

(LEFT INSIDE)

BEST AVAILABLE COPY

ASSISTANT COMMISSIONER FOR PATENTS

WASHINGTON, D.C. 20231

ATTENTION: BOX PATENT APPLICATION

Sir:

JC530 U.S. PTO
09/519829
03/06/00

Transmitted herewith for filing is the patent application of

Inventors: **Sten-Olov Engberg and Ake Jonsson**

For: **USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION**

Enclosed are:

(X) A Specification in 21 pages

(X) 11 sheets of drawing.

(X) An Information Disclosure Statement.

(X) A PTO Form 1449 with three (3) references.

(X) A return prepaid postcard.

CLAIMS AS FILED

FOR	NUMBER FILED	NUMBER EXTRA	RATE	FEE
Basic Fee			$690	$690.00
Total Claims	27 - 20 =	7 ×	$18	$126.00
Independent Claims	4 - 3 =	1 ×	$78	$78.00
If application contains any multiple dependent claims(s), then add			$260	$0

FILING FEE TO BE PAID AT A LATER DATE $894.00

(X) Please use Customer No. 20,995 for the correspondence address.

Jerry T. Sewell
Registration No. 31,567
Attorney of Record

JTS-4508.DOC:ke
20000306

KNOBBE, MARTENS, OLSON & BEAR, LLP
620 NEWPORT CENTER DR 16TH FLOOR NEWPORT BEACH, CA 92660
(949) 760-0404 FAX (949) 760-9502

INTELLECTUAL PROPERTY LAW

KNOBBE, MARTENS, OLSON & BEAR

A LIMITED LIABILITY PARTNERSHIP INCLUDING PROFESSIONAL CORPORATIONS

PATENT, TRADEMARK AND COPYRIGHT CAUSES

620 NEWPORT CENTER DRIVE

SIXTEENTH FLOOR

NEWPORT BEACH, CALIFORNIA 92660-8016

(949) 760-0404

FAX (949) 760-9502

INTERNET: WWW.KMOB.COM

LOUIS J. KNOBBE*
DON W. MARTENS*
GORDON H. OLSON*
JAMES B. BEAR
DARRELL L. OLSON*
WILLIAM B. BUNKER
WILLIAM H. NIEMAN
ARTHUR S. ROSE
JAMES F. LESNIAK
NED A. ISRAELSEN
DREW S. HAMILTON
JERRY T. SEWELL
JOHN B. SGANGA, JR.
EDWARD A. SCHLATTER
GERARD VON HOFFMANN
JOSEPH R. RE
CATHERINE J. HOLLAND
JOHN M. CARSON
KAREN VOGEL WEIL
ANDREW H. SIMPSON
JEFFREY L. VAN HOOSEAR
DANIEL E. ALTMAN
MARGUERITE L. GUNN
STEPHEN C. JENSEN
VITO A. CANUSO III
WILLIAM H. SHREVE
LYNDA J. ZADRA-SYMES†
STEVEN J. NATAUPSKY
PAUL A. STEWART
JOSEPH F. JENNINGS
CRAIG S. SUMMERS
ANNEMARIE KAISER
BRENTON R. BABCOCK

THOMAS F. SMEGAL, JR.
MICHAEL H. TRENHOLM
DIANE M. REED
JONATHAN A. BARNEY
RONALD J. SCHOENBAUM
JOHN R. KING
FREDERICK S. BERRETTA
NANCY WAYS VENSKO
JOHN P. GIEZENTANNER
ADEEL S. AKHTAR
GINGER R. DREGER
THOMAS R. ARNO
DAVID N. WEISS
DANIEL HART, PH.D.
DOUGLAS G. MUEHLHAUSER
LORI LEE YAMATO
MICHAEL K. FRIEDLAND
STEPHEN M. LOBBIN
STACEY R. HALPERN
DALE C. HUNT, PH.D.
LEE W. HENDERSON, PH.D.
DEBORAH S. SHEPHERD
RICHARD E. CAMPBELL
MARK M. ABUMERI
JON W. GURKA
ERIC M. NELSON
ALEXANDER C. CHEN
MARK R. BENEDICT, PH.D.
PAUL N. CONOVER
ROBERT J. ROBY
SABING H. LEE
KAROLINE A. DELANEY
JOHN W. HOLCOMB

JAMES J. MULLEN, III, PH.D.
JOSEPH S. CIANFRANI
JOSEPH M. REISMAN, PH.D.
WILLIAM R. ZIMMERMAN
GLEN L. NUTTALL
ERIC S. FURMAN, PH.D.
DO TE KIM
TIRZAH ABE LOWE
GEOFFREY Y. IIDA
ALEXANDER S. FRANCO
SANJIVPAL S. GILL
SUSAN M. MOSS
JAMES W. HILL, M.D.
ROSE M. THIESSEN, PH.D.
MICHAEL L. FULLER
MICHAEL A. GUILIANA
MARK J. KERTZ
RABINDER N. NARULA
BRUCE S. ITCHKAWITZ, PH.D.
PETER M. MIDGLEY
THOMAS S. MCCLENAHAN
MICHAEL S. OKAMOTO
JOHN M. GROVER
MALLARY K. MCCARTHY
IRFAN A. LATEEF
AMY C. CHRISTENSEN
SHARON S. NG
MARK J. GALLAGHER, PH.D.
DAVID G. JANKOWSKI, PH.D.
BRIAN C. HORNE
PAYSON J. LEMEILLEUR

OF COUNSEL
JERRY R. SEILER

JAPANESE PATENT ATTY
KATSUHIRO ARAI**

EUROPEAN PATENT ATTY
MARTIN HELLEBRANDT

KOREAN PATENT ATTY
MINCHEOL KIM

SCIENTISTS & ENGINEERS
(NON-LAWYERS)

RAIMOND J. SALENIEKS**
NEIL S. BARTFELD, PH.D.**
DANIEL E. JOHNSON, PH.D.**
JEFFERY KOEPKE, PH.D.
KHURRAM RAHMAN, PH.D.
JENNIFER A. HAYNES, PH.D.
BRENDAN P. O NEILL, PH.D.
THOMAS Y. NAGATA
ALAN C. GORDON
LINDA H. LIU
MICHAEL J. HOLIHAN
YASHWANT VAISHNAV, PH.D.
MEGUMI TANAKA

* A PROFESSIONAL CORPORATION
† ALSO BARRISTER AT LAW (U.K.)
** U.S. PATENT AGENT

Assistant Commissioner for Patents
Washington, D.C. 20231

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

Attorney Docket No.	:	APRILS.001A
Applicant(s)	:	Sten-Olov Engberg, et al.
For	:	USE OF PERSONAL COMMUNICATION DEVICE FOR USER AUTHENTICATION
Attorney	:	Jerry T. Sewell
"Express Mail" Mailing Label No.	:	EL 103 698 371 US
Date of Deposit	:	March 6, 2000

I hereby certify that the accompanying

Transmittal in Duplicate; Specification in 21 pages; 11 sheets of drawings; Information Disclosure Statement, PTO Form 1449 with three (3) references; Return Prepaid Postcard

are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and are addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Donald King

JTS-4507.DOC:ke
20000306

201 CALIFORNIA STREET
SUITE 1150
SAN FRANCISCO, CALIFORNIA 94111
(415) 954-4114
FAX (415) 954-4111

501 WEST BROADWAY
SUITE 1400
SAN DIEGO, CALIFORNIA 92101
(619) 235-8550
FAX (619) 235-0176

3801 UNIVERSITY AVENUE
SUITE 710
RIVERSIDE, CALIFORNIA 92501
(909) 781-9231
FAX (909) 781-4507

1875 CENTURY PARK EAST
SUITE 600
LOS ANGELES, CALIFORNIA 90067
(310) 407-5484
FAX (310) 407-5485

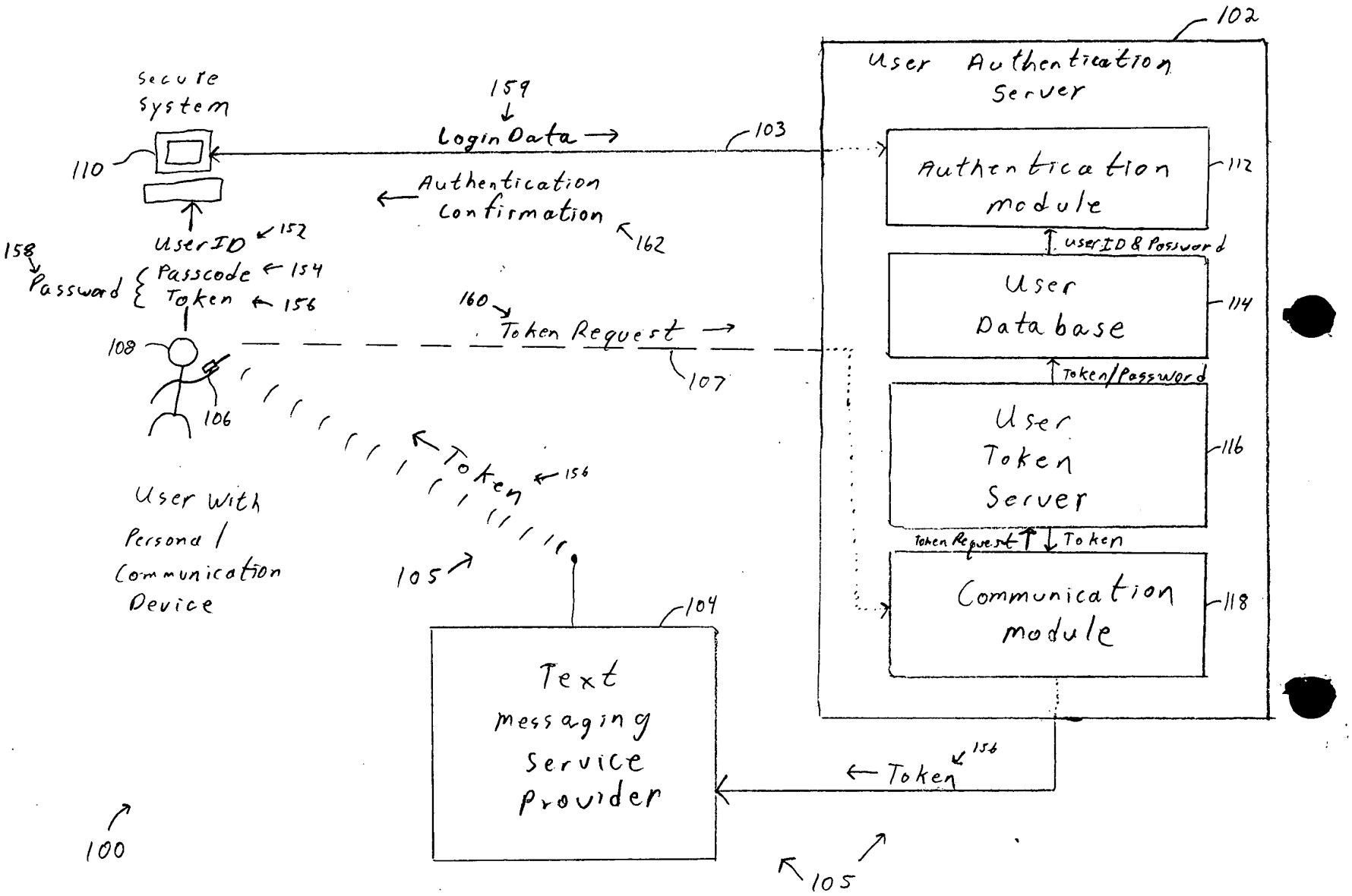

102
User Authentication Server
Secure System
159
Login Data
103
110
Authentication Confirmation
162
Authentication module
112
UserID
152
158
Password
Passcode
154
Token
156
UserID & Password
User Database
114
160
Token Request
108
107
Token/Password
User Token Server
116
106
Token
156
User with Personal Communication Device
Token Request
Token
105
Communication module
118
104
Text messaging service provider
Token
156
100
105

Fig 1

Logon To Network:

USERID

PASSWORD

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

Fig 2A

Logon To Network:

USERID

PASSCODE

TOKEN

Fig 2B

Please enter a user ID to request a Token.
Token will be instantly transmitted to your registered Personal Communication Device and will be valid for one minute.

USERID

Fig 2C

Logon To Network:

PASSCODE

TOKEN

Fig 2D

Confidential - Subject to Protective Order

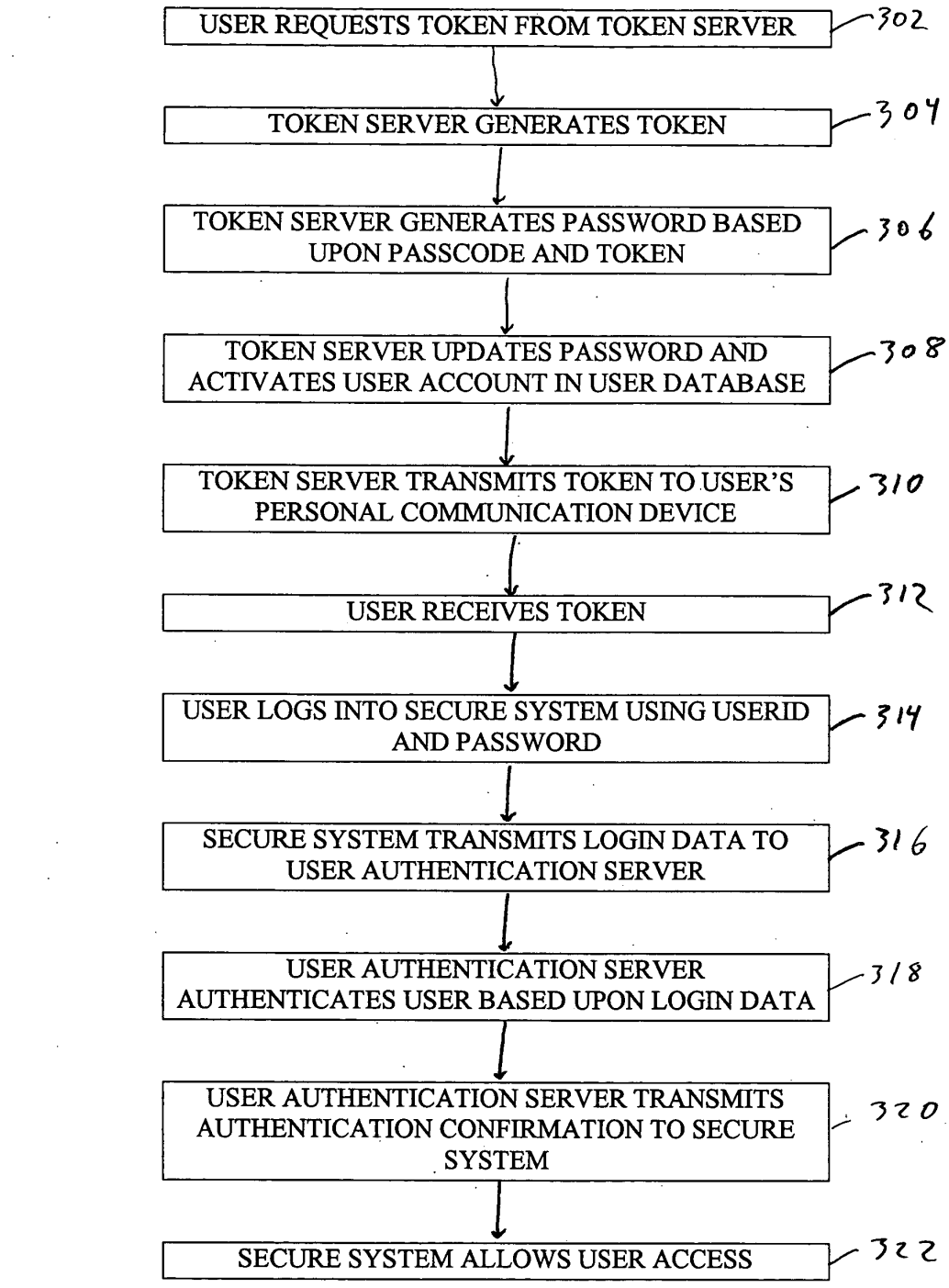

USER REQUESTS TOKEN FROM TOKEN SERVER
302
TOKEN SERVER GENERATES TOKEN
304
TOKEN SERVER GENERATES PASSWORD BASED UPON PASSCODE AND TOKEN
306
TOKEN SERVER UPDATES PASSWORD AND ACTIVATES USER ACCOUNT IN USER DATABASE
308
TOKEN SERVER TRANSMITS TOKEN TO USER'S PERSONAL COMMUNICATION DEVICE
310
USER RECEIVES TOKEN
312
USER LOGS INTO SECURE SYSTEM USING USERID AND PASSWORD
314
SECURE SYSTEM TRANSMITS LOGIN DATA TO USER AUTHENTICATION SERVER
316
USER AUTHENTICATION SERVER AUTHENTICATES USER BASED UPON LOGIN DATA
318
USER AUTHENTICATION SERVER TRANSMITS AUTHENTICATION CONFIRMATION TO SECURE SYSTEM
320
SECURE SYSTEM ALLOWS USER ACCESS
322
300

Fig 3

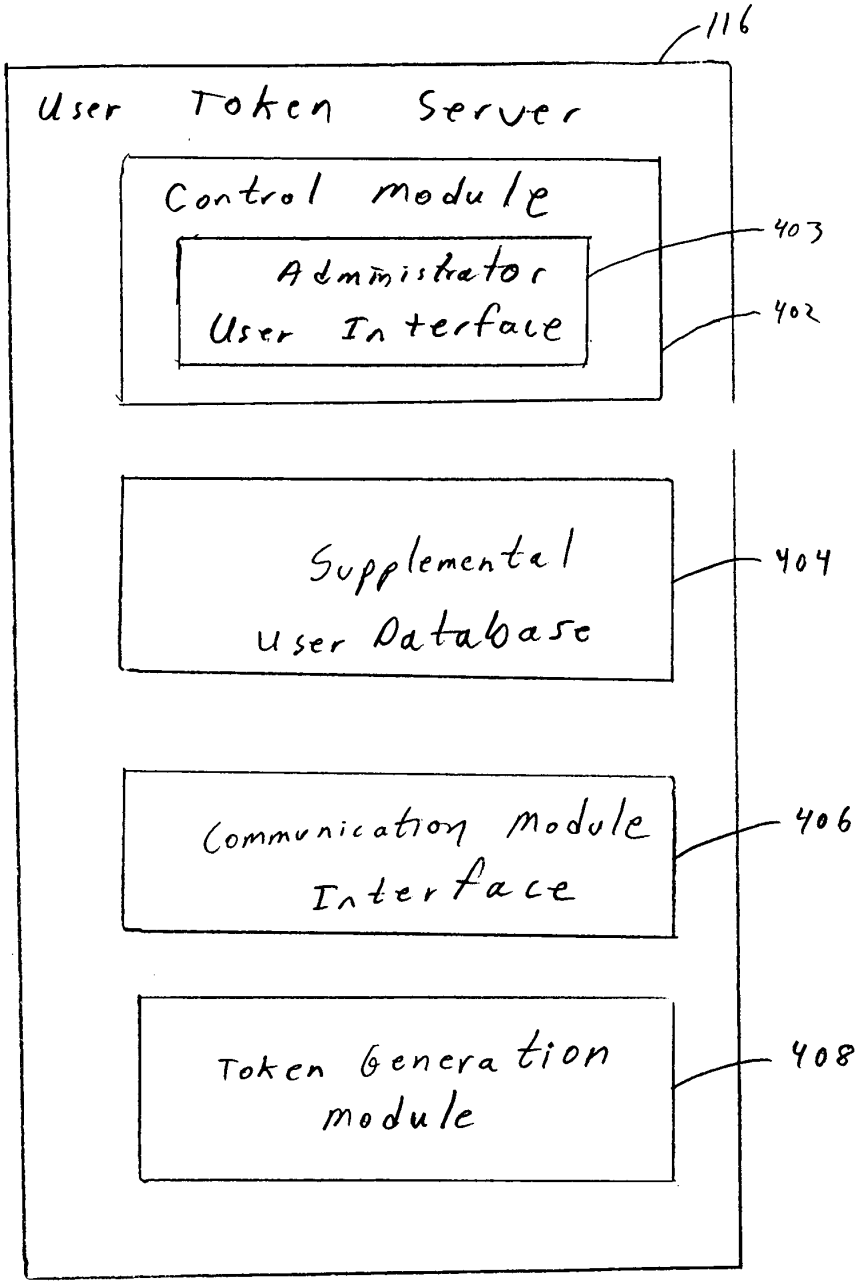
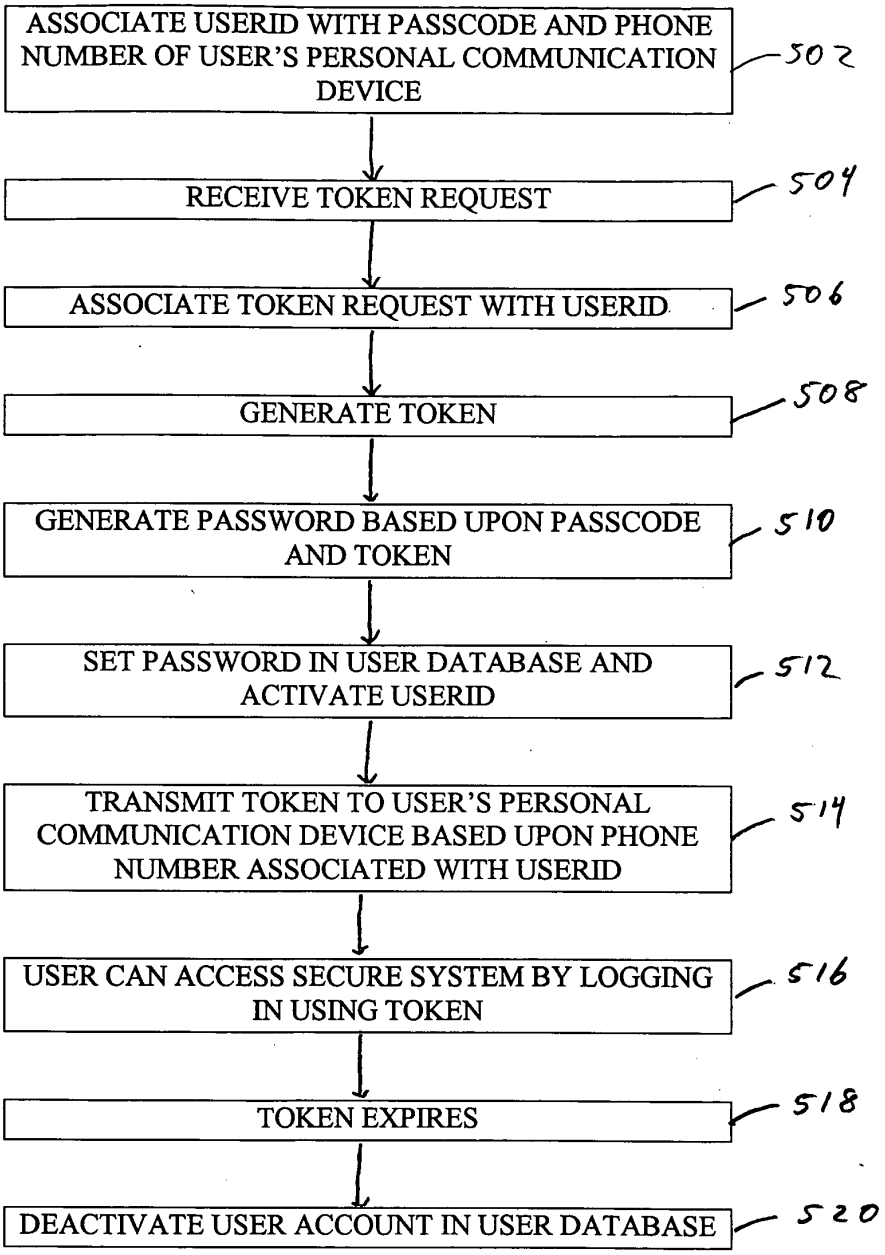

116
User Token Server
Control module
Administrator User Interface
403
402
Supplemental User Database
404
Communication module Interface
406
Token Generation module
408

Fig 4



500

Fig 5

Doc Code: Appeal Brief

0090E0" 6286T560

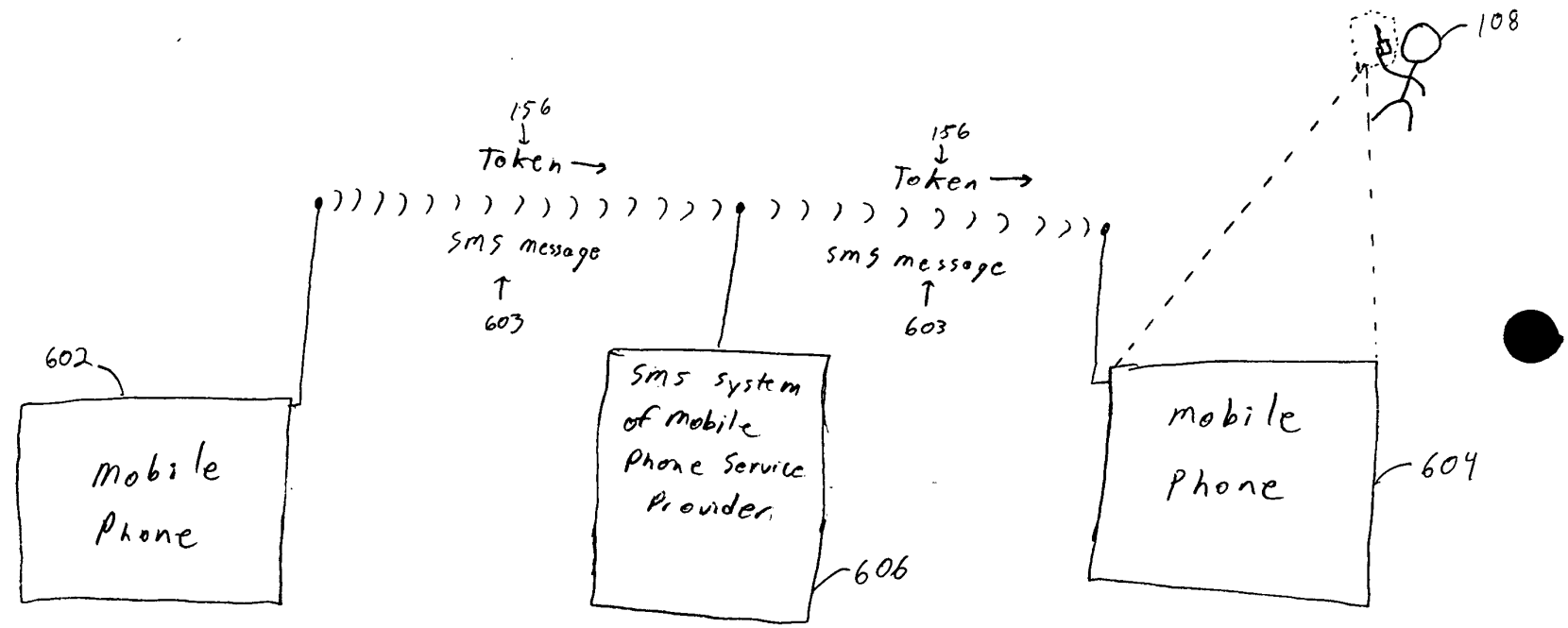


Fig 6A

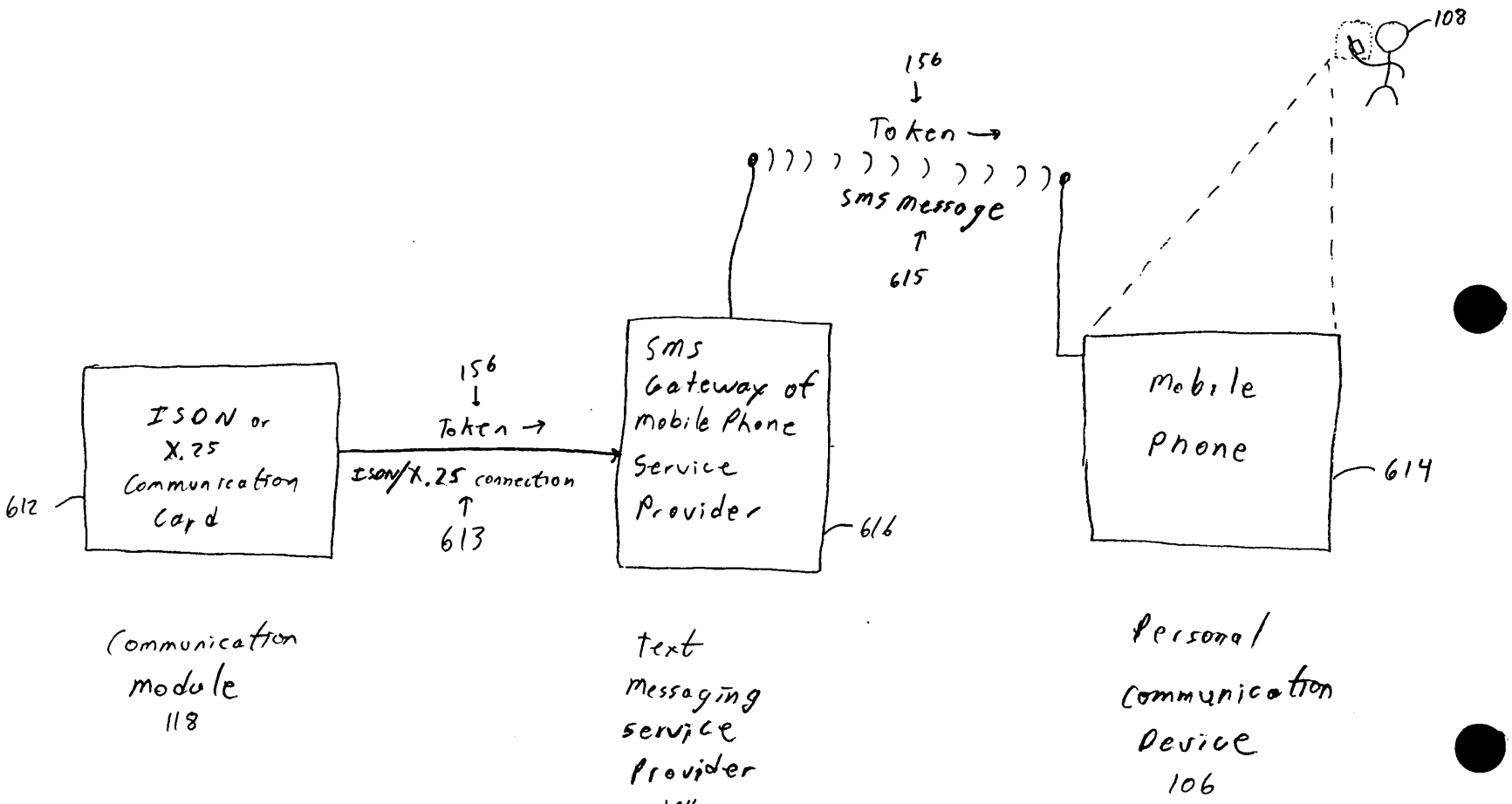

156
Token
SMS message
615
108
ISON or X.25 Communication Card
612
156
Token
ISON/X.25 connection
613
SMS Gateway of Mobile Phone Service Provider
616
Mobile Phone
614
Communication module 118
Text Messaging service Provider 104
Personal Communication Device 106
Token Delivery
105

Fig 6B

DOCKET 6286T560

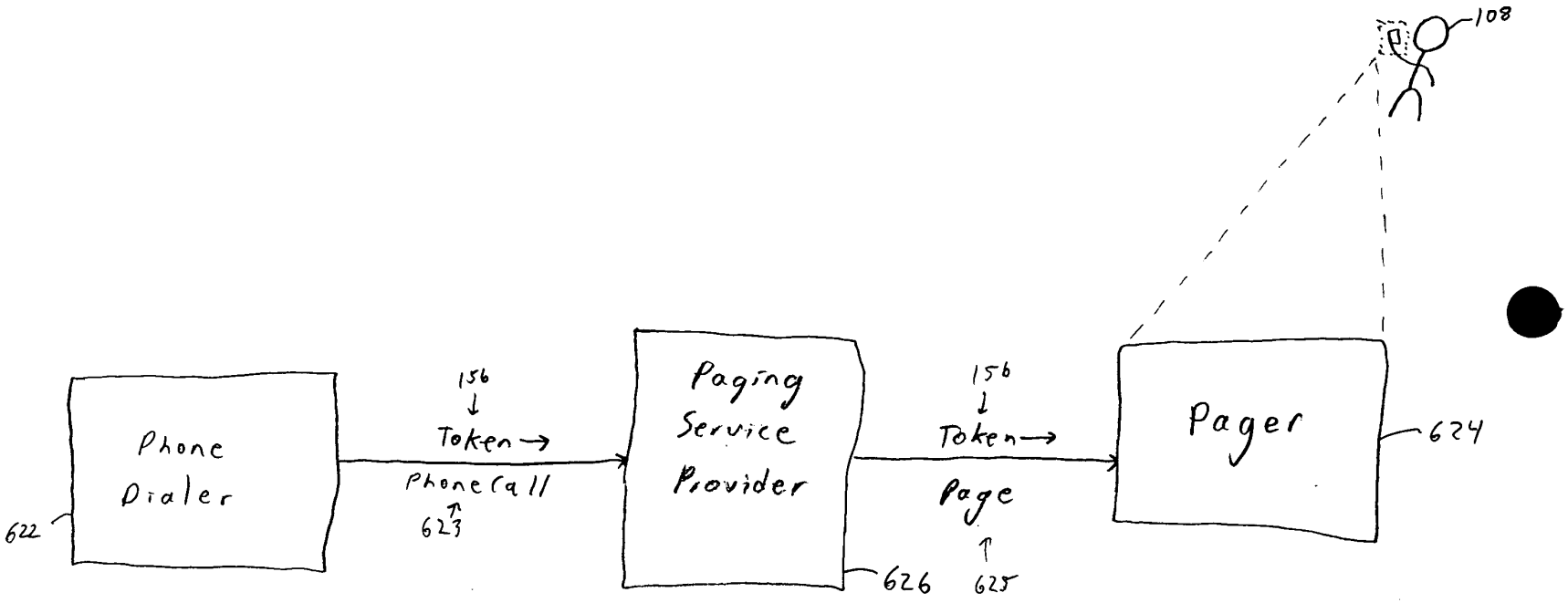


Fig 6C

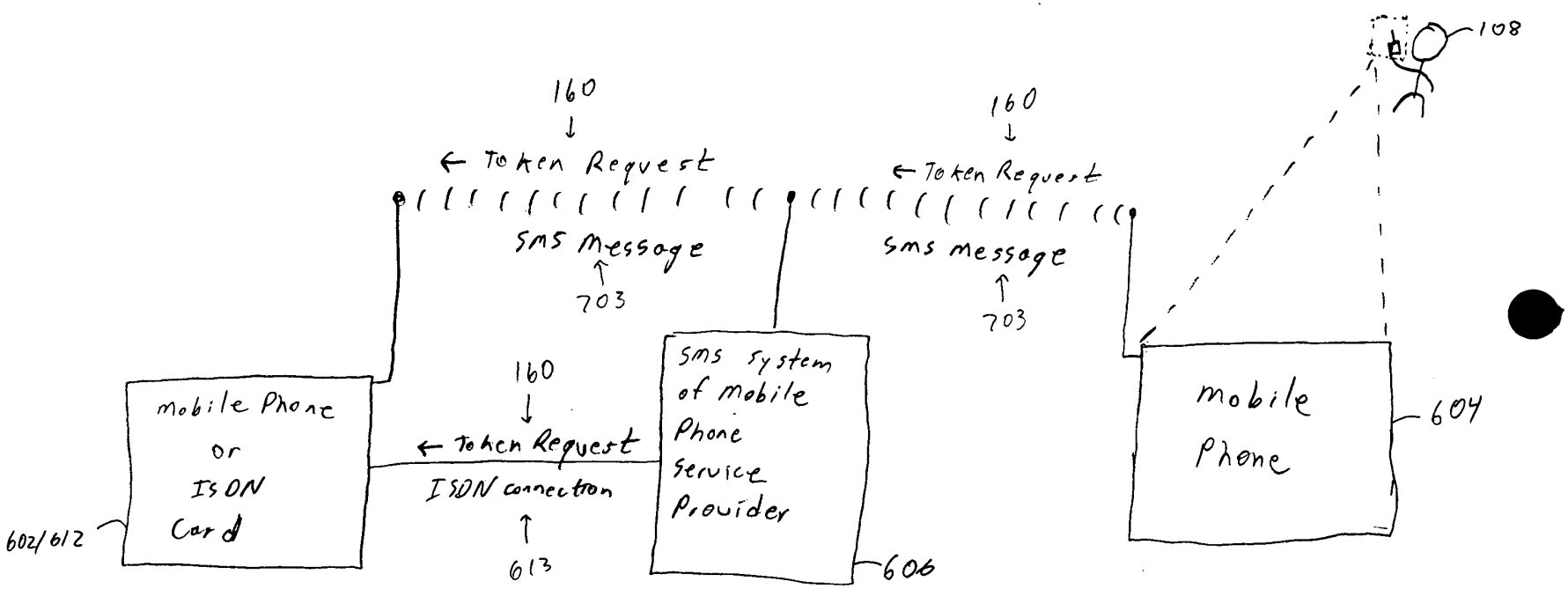
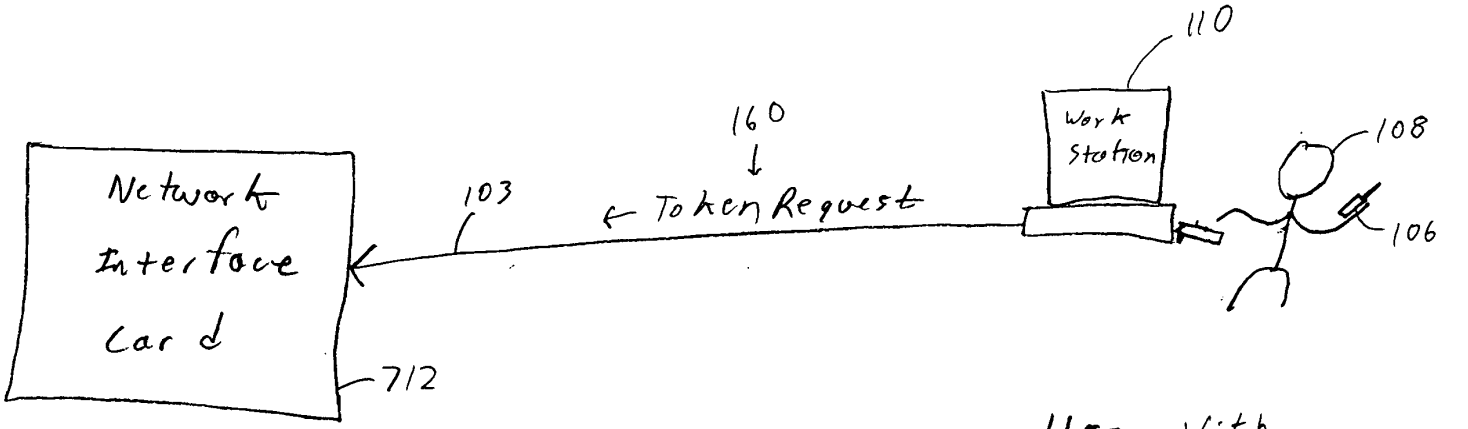

160
Token Request
SMS Message
703
160
Token Request
SMS Message
703
108
160
Token Request
ISDN connection
613
Mobile Phone or ISDN Card
602/612
SMS System of Mobile Phone Service Provider
606
Mobile Phone
604
Communication Module
118
Text Messaging Service Provider
104
Personal Communication Device
106
Token Request
107

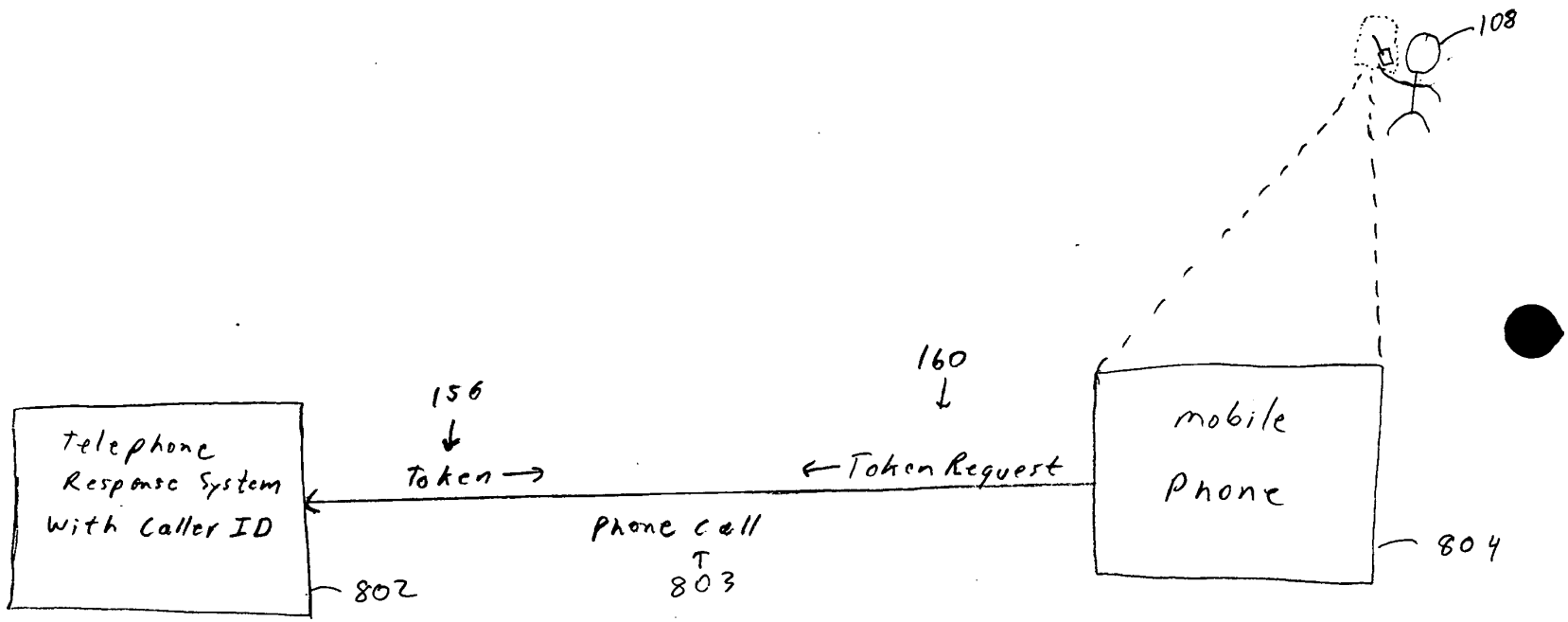
Fig 7A

09950"6286T560



Token Request 107

Fig 7B



Communication module 118

Personal Communication Device 106

Token Request and Delivery

Fig 8

USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION

Background of the Invention

Field of the Invention

This invention relates generally to the authentication of users of secure systems and, more particularly, the invention relates to a system through which user tokens required for user authentication are supplied through personal communication devices such as mobile telephones and pages.

Description of the Related Art

Secure systems have traditionally utilized a user ID and password pair to identify and authenticate system users. Operating systems that control local area networks of workstations within a business or institution such as Novell NetWare, Microsoft NT, Windows 2000, and UNIX/Linux typically require submission of a user ID and password combination before allowing access to a workstation.

The incorporation of remote connectivity to secure systems over the Internet has weakened traditional controls imposed by a user's required physical presence within a company's premises and has exposed systems to additional security threats. External users accessing by dial-in or over the Internet, complicated by frequent personnel turnover, require frequent changes in password lists.

Passwords created by users are often combinations of words and names, which are easy to remember but also easily guessed. Guessing passwords is a frequent technique used by "hackers" to break into systems. Therefore, many systems impose regulations on password formats that require mixtures of letters of different cases and symbols and that no part of a password be a word in the dictionary. A user's inability to remember complex combinations of letters, numbers, and symbols often results in the password being written down, sometimes on a note stuck to the side of a workstation.

Present systems face several problems: users dread frequent password changes, frequent password changes with hard-to-remember passwords inevitably result in users

surreptitiously writing down passwords, and security is compromised when users write down their passwords.

The SecurID product, which is distributed by RSA Security Inc., solves many of the aforementioned problems by requiring a two-factor authentication process. The first factor is a user passcode or personal identification number. The second factor is a SecurID card that is possessed by the user. The SecurID card generates and displays unpredictable, one-time-only access codes that automatically change every 60 seconds. The user supplies the displayed code upon logging into a system. The system has a corresponding code generator that allows verification of possession of the card.

The SecurID product, however, requires users to carry an additional item on their person in order to access a secure system. It 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 a mobile phone or a pager.

0508-0000 - 0503-0000

Summary of the Invention

A preferred embodiment of the present invention is a password setting system for setting user passwords for a secure system, such as a computer system or a secure area of a building. The password setting system preferably includes a user token server and a communication module. The user token server generates a random token in response to a request for a new password from a user. The server creates a new password by concatenating a secret passcode that is known to the user with the token. The server sets the password associated with the user's user ID to be the new password. The communication module transmits the token to a personal communication device, such as a mobile phone or a pager carried by the user. The user concatenates the secret passcode with the received token in order to form a valid password, which the user submits to gain access to the secure system. Accordingly, 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.

One aspect of the invention is a method for setting passwords. The method includes associating a user ID with a phone number of a personal communication

device. The method also includes generating a new password based at least upon a token. The method also includes setting a password associated with the user ID to be the new password. The method also includes transmitting the token to the personal communication device using the phone number associated with the user ID. In another aspect, the method also includes associating the user ID with a passcode. In another aspect, the new password is generated based additionally upon the passcode. In another aspect, the method also includes receiving a request for the user token. In another aspect, the personal communication device is a mobile phone. In another aspect, the personal communication device is a pager.

An additional aspect of the invention is a password setting system. The system includes a first user database configured to associate a user ID with a phone number of a personal communication device. The system also includes a control module configured to create a password based at least upon a token. The control module is further configured to cause a second user database to associate the password with the user ID. The system also includes a communication module interface configured to cause a communication module to transmit the token to the personal communication device using the phone number associated with the user ID. In another aspect, the first user database and the second user database are the same database. In another aspect, the first user database is further configured to associate the user ID with a passcode, and the control module is further configured to create the password based additionally upon the passcode.

An additional aspect of the invention is a method of regulating access to a secure system. The method includes transmitting a user token to a personal communication device. The method also includes receiving login data in response to a request for authentication information, wherein the login data is based at least upon the user token. The method also includes granting access to the secure system based upon the received login data. In another aspect, the login data is additionally based upon a user ID. In another aspect, the login data comprises a user ID. In another aspect, the login data is additionally based upon a passcode. In another aspect, the login data comprises a user ID and a password. In another aspect, the password comprises a passcode and the token. In another aspect, the password is a concatenation of the passcode and the token.

In another aspect, the password is a hashed concatenation of the passcode and the token. In another aspect the method also includes generating the user token. In another aspect the method also includes receiving a request for the user token. In another aspect, the personal communication device is a mobile phone. In another aspect, the personal communication device is a pager.

An additional aspect of the invention is an access control system. The system includes a user token server configured to transmit a token to a personal communication device. The user token server is further configured to generate a valid password based at least upon the token. The system also includes an authentication module configured to receive at least a submitted password in response to a request for authentication of a user. The authentication module is further configured to grant access to the user if at least the submitted password is based at least upon the token and matches the valid password. In another aspect, the user token server is further configured to generate the valid password based additionally upon a valid passcode that is known to the user. In another aspect, the user token server is further configured to transmit the token in response to a request by the user. In another aspect, the user token server is further configured to associate the valid password with a valid user ID, the authentication module is further configured to receive a submitted user ID in response to the request for authentication, and the authentication module is further configured to grant access to the user if, in addition, the submitted user ID matches the valid user ID.

Google Exhibit 1009

Brief Description of the Drawings

The present invention will be described below in connection with the attached drawings in which:

Figure 1 illustrates an overview, including system components, of a user authentication system according to a preferred embodiment of the present invention;

Figures 2A-D illustrate login screens that can be used in conjunction with various embodiments of the invention;

Figure 3 illustrates a preferred process performed by the system to authenticate users;

Figure 4 illustrates a preferred embodiment of a user token server;

Figure 5 illustrates a preferred process by which the user token server provides tokens and administrates user accounts;

Figures 6A-C illustrate three embodiments of a token delivery communication link;

Figures 7A-B illustrate two embodiments of a token request communication link; and

Figure 8 illustrates an embodiment of a combined token request and delivery communication link.

Detailed Description of the Embodiments

In the following description, reference is made to the accompanying drawings, which form a part hereof, and which show, by way of illustration, specific embodiments or processes in which the invention may be practiced. Where possible, the same reference numbers are used throughout the drawings to refer to the same or like components. In some instances, numerous specific details are set forth in order to provide a thorough understanding of the present invention. The present invention, however, may be practiced without the specific details or with certain alternative equivalent devices and methods to those described herein. In other instances, well-known methods and devices have not been described in detail so as not to unnecessarily obscure aspects of the present invention.

I. Overview and System Components

Figure 1 illustrates an overview, including system components, of a user authentication system 100 according to a preferred embodiment of the present invention. Figure 2A illustrates login screen that can be used in accordance with the preferred embodiment. Figures 2B-D illustrate a login screens that can be used in accordance with alternative embodiments.

The user authentication system 100 includes an authentication server 102, a text messaging service provider 104, a personal communication device 106 carried by a user 108, and a secure system 110 to which the authentication system 100 regulates access. The personal communication device 106 is preferably a pager or a mobile phone having SMS (short message service) receive capability. SMS is a secure text messaging

capability that is incorporated into most digital mobile phones. The secure system 110 is preferably a Windows NT computer workstation, but may be any system, device, account, or area to which it is desired to limit access to authenticated users. The secure system 110 may be, for example, a user account on a network of computer workstations, a user account on a web site, or a secure area of a building. The secure system 110 is preferably connected to the user authentication server 102 by a computer network 103. In one embodiment, the user authentication server 102 is integrated into the secure system 110.

The user authentication server 102 preferably includes a program or a suite of programs running on a computer system to perform user authentication services. The user authentication server 102 may also include the computer system and hardware upon which the programs run. The user authentication server 102 is preferably configured to require that the user 108 supply authentication information through the secure system 110 in order to gain access to the secure system 110.

The authentication information preferably includes a user ID 152, a passcode 154 and a user token 156. The user 108 preferably commits to memory the user ID 152 and passcode 154. The user ID 152 may be publicly known and used to identify the user 108. The passcode 154 is preferably secret and only known to the user 108. The token 156 is preferably provided only to the user 108 by the user authentication server 102 through the user's personal communication device 106 on an as needed basis. The token 156 preferably has a limited lifespan, such as 1 minute or 1 day. Accordingly, the user 108 needs to be in possession of his personal communication device 106 in order to gain access to the secure system 110. Therefore, if the user's user ID 152 and passcode 154 are compromised, a malicious party still cannot access the secure system without possession of the personal communication device 106.

In the preferred embodiment, the user 108 combines the token 156 with the passcode 154 to form a password 158. For example, the user 108 can combine a valid, memorized passcode of "abcd" with a valid token of "1234" to form a valid password of "abcd1234." In this manner, a login screen such as is illustrated in Figure 2A, which is similar or identical to standard login screens that require a user ID 152 and a password 158, can be used. In an alternative embodiment, the passcode 154 and the token 156 are

submitted separately, as is illustrated in Figure 2B. In another embodiment, the passcode 154 is null in which case the token 156 alone is used as the password 158. In still another embodiment, the token 156 can be requested through the secure system 110 as is illustrated in Figures 2C-D.

The user authentication server 102 is preferably a secure system itself and may be a part or component of the secure system 110. The user authentication server 102 preferably includes an authentication module 112 and a user database 114. The authentication module 112 is preferably identical to the code or software provided with operating systems such as Windows NT that authenticates users upon login. In alternative embodiments, the authentication module 112 may be any code, device, or module capable of 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. The authentication module 112 preferably responds to an authentication request transmitted over the computer network 103 by supplying an authentication confirmation 162 over the network 103. If the user 108 has been authenticated, the confirmation 162 instructs the secure system 110 to allow access to the user 108. The user database 114 is preferably similar or identical to the database accessed by the authentication module 112 that stores user ID and password data (or passcode and token data) in operating systems such as Windows NT. In alternative embodiments, the user database 114 can be any database capable of storing user ID and password data.

The user authentication server 102 preferably also includes a user token server 116 that responds to requests for tokens 160 by generating a token 156 and transmitting the token 156 to the user's personal communication device 106. The user authentication server 102 preferably also resets passwords in the user database 114 based upon generated tokens and passcode data. The user authentication server 102 preferably transmits the tokens 156 over a token delivery communication link 105 to the user's personal communication device 106.

The user authentication server 102 preferably also includes a communication module 118, which is also part of the token delivery communication link 105. The communication module 118 forwards tokens 156 to a text messaging service provider 104, which may be a pager or mobile phone service provider. The text messaging

service provider 104 then forwards the token 156 preferably in the form of a secure text message to the personal communication device 106.

In the preferred embodiment, the communication module 118 is a mobile phone with SMS text messaging send capability. One applicable mobile phone is the presently available Ericsson T-28. The mobile phone 118 is preferably connected to the user authentication server 102 via a presently available serial port cable that makes the phone accessible in a manner similar to a computer modem. Accordingly, the user authentication server 102 can send tokens 156 via the server's mobile phone 118 to the user's mobile phone 106 using SMS. In this case, the server's mobile phone 118 transmits a message including the token 156 to the user's personal communication device 106 using the phone number of the user's personal communication device 106. During the transmission, the message is relayed by the mobile phone service provider 104 to its final destination.

Preferably, the communication module 118 is also configured to receive requests for tokens 160. The user preferably transmits a request for tokens 160 over a request communication link 107. The request communication link 107 may be the same communication link as the delivery communication link 105 or it may be a different link. Various embodiments of the token delivery communication link 105 and the token request communication link 107 will be discussed in Section III below.

In the preferred embodiment, the communication module 118 is a mobile phone that also has SMS text messaging receive capability. The communication module 118 receives an SMS message from the user's mobile SMS send enabled mobile phone 106, and the token server 116 preferably processes the message as a token request 160. The incoming SMS message is tagged with the sending phone's phone number, which the user token server 116 can use to identify the requesting user and respond with a new token 156. The token request 160 may also be in the form of a phone call, in which case the user token server 116 may use a caller ID feature to identify the calling phone number as a valid user's personal communication device 106. The user token server 116 can then respond with a new token 156. Alternatively, the user token server 116 may allow a calling user 108 to enter the phone number of his personal communication device 106 using the mobile phone keypad once a connection has been established.

In an alternative embodiment, the communication module 118 is an ISDN card that is connected to the text messaging service provider 104 preferably via an X.25 connection. The ISDN card 118 preferably transmits new tokens directly to the text messaging service provider 104 for forwarding to the user's personal communication device 106. The ISDN card 118 may also be configured to be accessible at a phone number to receive calls for requests for tokens 160.

Figure 3 illustrates a preferred process 300 performed by the system 100 to authenticate users. At a step 302, the user 108 requests a token from the user token server 116 through the token request communication link 107. In the preferred embodiment, the user's mobile phone 106 has SMS send capability and the user sends an SMS message to the communication module 118 requesting a new token 156. The SMS message need not contain any data in its body since the phone number of the sending mobile phone is automatically sent along with the message. The user token server 116 preferably identifies the user's mobile phone 106 based upon the phone number with which the SMS message is tagged. In an alternative embodiment, the user 108 makes a phone call with his personal communication device 106 to the communication module 118. The user token server 116 identifies the user's personal communication device 106 preferably based upon a caller ID feature. Alternatively, the user 108 may call from any phone and enter in the phone number of his personal communication device 106. As another alternative, the user 108 may request the token 156 through the secure system 110 itself as illustrated in Figures 2C-D. As another alternative, the step 302 may be omitted altogether. In this case, the user token server 116 can automatically send tokens 156 to the user 108 at predetermined intervals, such as once per day where the tokens have a lifespan of one day.

At a step 304 the user token server 116 generates a token 156. The token 156 may be generated by any of a number of methods that preferably produces a random or pseudo-random sequence of numbers and/or digits. The token 156 is preferably long enough such that it cannot be guessed, but short enough such that it is relatively easy to enter, such as six to eight characters.

At a step 306, the token server 116 generates a new password 158. The token server 116 preferably creates the new password 158 by combining the user's passcode

154, which is stored by the user token server 116, with the newly generated token 156. At a step 308, the token server updates the user database 114 with the new password 158. In the case that the user's account in the user database 114 is inactive or deactivated, the token server 116 activates the user's account.

In the preferred embodiment, the token server creates a hash of the password 158 and stores the hash of the password 158 in the user database 114 rather than storing the password 158 itself. The hash is typically performed using a one-way hashing algorithm where the same password always produces the same hash, but where the password cannot be determined from the hash. In typical systems, passwords 158 are stored as hashes rather than as plain text in order to prevent system administrators and others from being able to determine users' passwords by examining the user database 114. Also, when a user 108 submits a password 158 upon login to a secure system 110, the submitted password 158 is immediately hashed using the same one-way hashing algorithm before transmission to the authentication module 112. The authentication module 112 then compares hashes of passwords rather than the passwords themselves to authenticate the user 108. In this manner, passwords 158 need not be transmitted over any communication links or computer networks as clear text. It will be apparent to one skilled in the art that the present invention can be implemented with or without the hashing of passwords and that incorporating hashing of passwords does not substantively affect the scope or spirit of the invention. So as not to unnecessarily obscure aspects of the present invention, a password as referred to herein may be an unhashed or a hashed password. For example, a receipt of a password may be a receipt of an unhashed or hashed password, and a comparison of passwords may be a comparison of unhashed or hashed passwords.

At a step 310, the token server 116 transmits the token 156 to the user's personal communication device 106 via the token delivery communication link 105. In the preferred embodiment, the communication module 118 is a mobile phone, and the user token server 116 uses the SMS send capability of the phone 118 to send an SMS message including the token 156 to the user's personal communication module 106. At a step 312, the user 108 receives the token through his personal communication device 106.

At a step 314, the user 108 logs into the secure system 110 using the user ID 152 and the password 158. In the preferred embodiment, the user 108 combines the passcode 154 and the token 156 by concatenation to form the password 158. In an alternative embodiment, the passcode 154 and the token 156 are submitted separately.

At a step 316, the secure system 110 transmits login data 159 to the user authentication server 102 over the computer network 103 for authentication of the user 108. The login data 159 preferably includes the user ID 152 and a hash of the password 158 that the secure system 110 creates in order to avoid sending the password 158 over the computer network 103 in clear text. Alternatively, the login data 159 may include a hash of the passcode 154 and the token 156. As another alternative, the password 158, or the passcode 154 and token 156 are not hashed.

At a step 318, the user authentication server 102 authenticates the user 108 based upon the login data 159. In order to authenticate the user 108, 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.

At a step 320, the user authentication server 102 transmits an authentication confirmation 162 to the secure system 110. At a step 322, the secure system 110 allows the user 108 access based upon the authentication confirmation 162.

II. The User Token Server

Figure 4 illustrates a preferred embodiment of the user token server 116. The user token server 116 preferably includes a process or program running on or in conjunction with the user authentication server 102. The user token server 116 may, however, include a computer upon which the process or program executes. The user token server 116 preferably includes a control module 402, a supplemental user database 404, a communication module interface 406, and a token generation module 408. The various modules and components of the user token server 116 are described herein from a functional perspective. The various functional components may, however, be seamlessly integrated into one or more executable programs, data structures, and/or physical components.

The control module 402 preferably serves as the top level component of the user token server 116. The control module 402 preferably handles any tasks or functions not handled by the other modules of the token server 116, in addition to controlling the other modules. The control module 402 preferably maintains a supplemental user database 404, which preferably stores associations of user IDs with passcodes, phone numbers of users' personal communication devices, and any other supplemental user data. The other supplemental user data may include one or more of: whether an account is active, the expiration time of passwords, and the frequency with which tokens may be automatically distributed. The supplemental user database 404 is preferably accessed and modified through an administrator user interface 403 provided by the control module 402. The administrator user interface 403 allows administration of user privileges by adding, modifying and removing user IDs, passcodes, and phone numbers from the supplemental user database 404.

In the preferred embodiment, the supplemental user database 404 is maintained separately from the user database 114 of the user authentication server 102. In this configuration, the user database 114 supplied with an OEM system need not be modified or reconfigured. The user token server 116 can be added to existing secure systems in order to provide additional security functionality. In an alternative embodiment, the supplemental user database 404 may be integrated into the user database 114. In this case, user authentication module 102 is preferably configured and supplied as a single integrated component.

Figure 5 illustrates a preferred process 500 by which the user token server 116 provides tokens 156 and administers user accounts. The process 500 is described below in conjunction with the description of the functionality of the various modules and components of the user token server 116.

At a step 502, the control module 402 associates a user ID with a passcode 154 and a phone number of a user's personal communication device 106. Upon initially setting up an account, the association can be performed manually by a system administrator through the administrator user interface 403. The administrator user interface 403 preferably solicits a desired user ID 152, passcode 154, and phone number from a system administrator. The control module 402 then preferably creates a

deactivated user account with a user ID 152 for the secure system 110 on the user database 114 of the user authentication server 102. The control module 402 preferably accesses the user database 114 using an application program interface (API) (not illustrated), which is typically provided with OEM systems. The control module 402 also preferably creates an entry in the supplemental user database 404 including the user ID 152, the passcode 154, and the phone number.

At a step 504, the user token server 116 receives a token request 160 from the user 108, possibly in order to activate his deactivated account. The token request 160 is preferably received through the communication module 118, which the control module 402 preferably controls through a communication module interface 406. The communication module interface 406 is preferably a device driver tailored for the specific implementation of the communication module 118. In alternative embodiments, the user may request the token 156 through the secure system 110 itself, as illustrated in Figures 2C-D. In this case, the request 160 may be received through the computer network 103.

At a step 506, the control module 402 associates the token request 160 with a valid user ID 152. The control module 402 may make this association based upon a supplied phone number by querying the supplemental user database 404. In one embodiment, if the user ID 152 is supplied in conjunction with the request 160, the step 506 is not performed .

At a step 508, the token generation module 408 generates a token by a method that produces a random or pseudo-random sequence of numbers or digits or both numbers and digits. Many methods are presently known for producing such random sequences. The token generation module 408 preferably passes the newly generated token 156 to the control module 402.

At a step 510, the control module 402 generates a new password 158 based upon the generated token 156 and the passcode 154 associated with the user ID 152 as listed in the supplemental user database 404. The new password 158 is preferably generated by concatenating the passcode 154 and the token 156.

At a step 512, the control module 402 sets or resets the password associated with the user ID 152 in the user database 114. In the preferred embodiment, the control

module 402 sets the password to be a one-way hash of the newly generated password 158. In alternative embodiments, the password 158 need not be hashed. In the case the user's account has been deactivated, the control module 402 activates the user ID 152 in the user database 114. The control module 402 preferably accesses the user database 114 through the database API (not illustrated).

At a step 514, the control module 402 transmits the token 156 to the user's personal communication device 106 preferably based upon the phone number associated with the user ID 152 in the supplemental user database 404. In the preferred embodiment, the control module 402 causes the communication module 118 to generate and send an SMS message containing the token 156 to the user's mobile phone. In an alternative embodiment, the communication module 118 may call the phone number of the user's pager and transmit the token 156 as the page data.

At a step 516, the user 108 is able to access the secure system 110 by logging in using the supplied token 156. The user 108 preferably concatenates his memorized secret passcode 154 with the valid token 156 to create the password 158. The user then logs in using his user ID 152 and the password 158.

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.

Finally, the process 500 repetitively continues either from the step 502, if a new user 108 is to be added, or from the step 504 if an existing user 108 requests a token 156.

III. Token Delivery and Request Communication Links

Figures 6A-C illustrate three embodiments of the token delivery communication link 105. Figures 7A-B illustrate two embodiments of the token request communication link 107. In some embodiments, the same communication link may be used as the token delivery communication link 105 and the token request communication link 107. Figure 8 illustrates an embodiment of a combined token request and delivery communication link that can function in conjunction with a mobile phone without text messaging capability. Additionally, communication technologies other than those

illustrated here by example may be used to implement the communication links 105 and 107.

Figure 6A illustrates a preferred embodiment of the token delivery communication link 105. The communication module 118 is a mobile phone 602 with SMS send capability. The mobile phone 602 sends an SMS message 603 including the token 156 to the user's mobile phone 604. While in transit, the message 603 is received and retransmitted by the SMS system 606 of a mobile phone service provider.

Figure 6B illustrates a first alternative embodiment of the token delivery communication link 105. In this case, the communication module 118 is an ISDN card or an X.25 connection card 612 that connects to an SMS gateway 616 of a mobile phone service provider via an ISDN or X.25 connection 613. The card 612 transmits the token 156 to the SMS gateway 616, which then creates an SMS message 615 and transmits the message 615 to the user's mobile phone 614.

Figure 6C illustrates a second alternative embodiment of the token delivery communication link 105. 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. The paging service provider 626 answers and the phone dialer 622 enters a numeric token 156 to be transmitted to the pager 624. The paging service provider 626, in turn, sends a page 625 containing the token 156 to the user's pager 624.

Figure 7A illustrates a preferred embodiment of the token request communication link 107. The personal communication device 106 is preferably the mobile phone 604, the communication module 118 is preferably the mobile phone 602, and the text messaging service provider 104 is preferably the SMS system 606 of the preferred embodiment of the token delivery communication link 105 (Figure 6A). Alternatively, the communication module 118 may be the ISDN card or X.25 connection card 612 connected through the ISDN or X.25 connection 613 as in the first alternative embodiment of the token delivery communication link 105 (Figure 6B). The mobile phone 604 preferably sends an SMS message 703 as a token request 160 to the mobile phone 602 or the ISDN card 612. The SMS message 703 may have a blank

message body but the message preferably includes the sending phone's phone number in a tag or header field. While in transit, the message 603 is received and retransmitted by the SMS system 606. The user token server 116 preferably identifies the sending phone's phone number, and if the phone number matches a valid user ID 152, the token server 116 processes the message 703 as a token request 160.

Figure 7B illustrates a first alternative embodiment of the token request communication link 107 in accordance with the token request and login screens of Figures 2C-D. The user 108 makes the token request 160 through a first login screen (Figure 2C) on the secure system 110. The token request 160 in this case preferably includes the user's user ID 152 and is preferably transmitted through the computer network 103 to the user token server 116 through a network interface card 702. In this case, the token request 160 need not be communicated through the communication module 118. Also, the personal communication device 106 need not be used in requesting the token 156 but is preferably used in delivering the token 156.

Figure 8 illustrates a combined token request and delivery link in which the personal communication device 106 is preferably a mobile phone. The communication module 118 is preferably an automated telephone response system 802 with a caller ID capability. The user 108 places a phone call 803 to the telephone response system 802, which identifies the calling phone 804 using caller ID. The telephone response system 802 interprets the call as a token request 160 and responds by generating a voice synthesized recitation of the token 156 that the user hears through the mobile phone 804. The mobile phone 804, in this case, need not have any text messaging or SMS capability.

In still other embodiments, various other technologies and combinations of technologies, which will be apparent to one skilled in the art, can be used to implement the token delivery 105 and token request 107 communication links. For example, a token request may be made through a land line phone, and in response, a token may be delivered to a mobile phone.

IV. Conclusion

Although the invention has been described in terms of certain preferred embodiments, other embodiments that are apparent to those of ordinary skill in the art,

including embodiments which do not provide all of the features and advantages set forth herein, are also within the scope of this invention. Accordingly, the scope of the invention is defined by the claims that follow. In the claims, a portion shall include greater than none and up to the whole of a thing; encryption of a thing shall include encryption of a portion of the thing; a password may be an unhashed or a hashed password. In the method claims, reference characters are used for convenience of description only, and do not indicate a particular order for performing the method.

0304304-000003

WHAT IS CLAIMED IS:

1. A method for setting passwords comprising:

(A) associating a user ID with a phone number of a personal communication device;

(B) generating a new password based at least upon a token;

(C) setting a password associated with the user ID to be the new password; and

(D) transmitting the token to the personal communication device using the phone number associated with the user ID.

2. The method of Claim 1, further comprising

(E) associating the user ID with a passcode.

3. The method of Claim 2, wherein (B) is based additionally upon the passcode.

4. The method of Claim 1, further comprising

(F) receiving a request for the user token.

5. The method of Claim 4, wherein (B), (C), and (D) are performed in response to (F).

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

7. The method of Claim 1, wherein the personal communication device is a pager.

8. A password setting system comprising:

a first user database configured to associate a user ID with a phone number of a personal communication device;

a control module configured to create a password based at least upon a token, the control module further configured to cause a second user database to associate the password with the user ID; and

a communication module interface configured to cause a communication module to transmit the token to the personal communication device using the phone number associated with the user ID.

9. The password setting system of Claim 8, wherein the first user database and the second user database are the same database.

10. The password setting system of Claim 8, wherein the first user database is further configured to associate the user ID with a passcode, and wherein the control module is further configured to create the password based additionally upon the passcode.

11. A method of regulating access to a secure system, the method comprising:

(A) transmitting a user token to a personal communication device;

(B) receiving login data in response to a request for authentication information, wherein the login data is based at least upon the user token; and

(C) granting access to the secure system based upon the received login data.

12. The method of Claim 11, wherein the login data is additionally based upon a user ID.

13. The method of Claim 11, wherein the login data comprises a user ID.

14. The method of Claim 12, wherein the login data is additionally based upon a passcode.

15. The method of Claim 11, wherein the login data comprises a user ID and a password.

16. The method of Claim 15, wherein the password comprises a passcode and the token.

17. The method of Claim 16, wherein the password is a concatenation of the passcode and the token.

18. The method of Claim 16, wherein the password is a hashed concatenation of the passcode and the token.

19. The method of Claim 11, further comprising

(D) generating the user token.

20. The method of Claim 19, further comprising

(E) receiving a request for the user token.

21. The method of Claim 20, wherein (A) and (D) are performed in response to (E).

22. The method of Claim 11, wherein the personal communication device is a mobile phone.

23. The method of Claim 11, wherein the personal communication device is a pager.

24. An access control system comprising:

a user token server configured to transmit a token to a personal communication device, the user token server further configured to generate a valid password based at least upon the token; and

an authentication module configured to receive at least a submitted password in response to a request for authentication of a user, the authentication module further configured to grant access to the user if at least the submitted password is based at least upon the token and matches the valid password.

25. The access control system of Claim 24, wherein the user token server is further configured to generate the valid password based additionally upon a valid passcode that is known to the user.

26. The access control system of Claim 24, wherein the user token server is further configured to transmit the token in response to a request by the user.

27. The access control system of Claim 25, wherein the user token server is further configured to associate the valid password with a valid user ID, wherein the authentication module is further configured to receive a submitted user ID in response to the request for authentication, and wherein the authentication module is further configured to grant access to the user if, in addition, the submitted user ID matches the valid user ID.

Add B1

USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION

Abstract of the Disclosure

A password setting system for a secure system includes a user token server and a communication module. The user token server generates a random token in response to a request for a new password from a user. The server creates a new password by concatenating a secret passcode that is known to the user with the token. The server sets the password associated with the user's user ID to be the new password. The communication module transmits the token to a personal communication device, such as a mobile phone or a pager carried by the user. The user concatenates the secret passcode with the received token in order to form a valid password, which the user submits to gain access to the secure system. Accordingly, 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.

H:\DOCS\ASF\ASF-1351.DOC
030600

Bib Data Sheet

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

SERIAL NUMBER	FILING DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
09/519,829	03/06/2000 RULE _	713	2777	APRILS.001A

APPLICANTS

Sten-Olov Engberg, Storvreta, SWEDEN;
Ake Jonsson, Fagersta, SWEDEN;

** CONTINUING DATA **********

** FOREIGN APPLICATIONS **********

IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** SMALL ENTITY **
** 04/14/2000

Foreign Priority claimed	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ yes ☒ no	SWEDEN	11	27	4
35 USC 119 (a-d) conditions met ☐ yes ☒ no ☐ Met after Allowance				
Verified and Acknowledged Examiner's Signature 12/4/00 Initials				

ADDRESS

20995

TITLE

Use personal communication devices for userauthentication

FILING FEE RECEIVED		
614	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

This Form is for INTERNAL PTO USE ONLY
It do[redacted]NOT get mailed to the a[redacted]licant.

NOTICE OF FILING / CLAIM FEE(S) DUE (CALCULATION SHEET)

APPLICATION NUMBER: _____

Total Fee Calculation

	Fee Code	Total # Claims		Number Extra	X	Fee Sm Entity	Fee Lg Entity	= Total
	Sm / Lg							
Basic Filing Fee	201 101						690	
Total Claims >20	202 102	27	-20 =	7	X		126	
Independent Claims >3	202 102	4	-3 =	1	X		78	
Mult Dep Claim Present	204 104							
Surcharge	205 105						130	
English Translation	139							
TOTAL FEE CALCULATION								

Fees due upon filing the application

Total Filing Fees Due = $ 1024

Less Filing Fees Submitted - $ _____

BALANCE DUE = $ 1024

Office of Initial Patent Examination

Figure 7

FORM OIPE-RAM-01 (Rev. 12/97)

PATENT APPLICATION FEE DETERMINATION RECORD
Effective December 29, 1999

Application or Docket Number

CLAIMS AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA
BASIC FEE		
TOTAL CLAIMS	27 minus 20=	* 7
INDEPENDENT CLAIMS	4 minus 3 =	* 1
MULTIPLE DEPENDENT CLAIM PRESENT		

SMALL ENTITY TYPE ☐		OR	OTHER THAN SMALL ENTITY	
RATE	FEE		RATE	FEE
	345.00	OR		690.00
X$ 9=		OR	X$18=	126
X39=		OR	X78=	78
+130=		OR	+260=	
TOTAL		OR	TOTAL	894

* If the difference in column 1 is less than zero, enter "0" in column 2

CLAIMS AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 26	Minus	** 27	=
Independent	* 5	Minus	*** 4	= 1
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X40 39=	40	OR	X78=	
+130=		OR	+260=	
TOTAL ADDIT. FEE	40	OR	TOTAL ADDIT. FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X39=		OR	X78=	
+130=		OR	+260=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

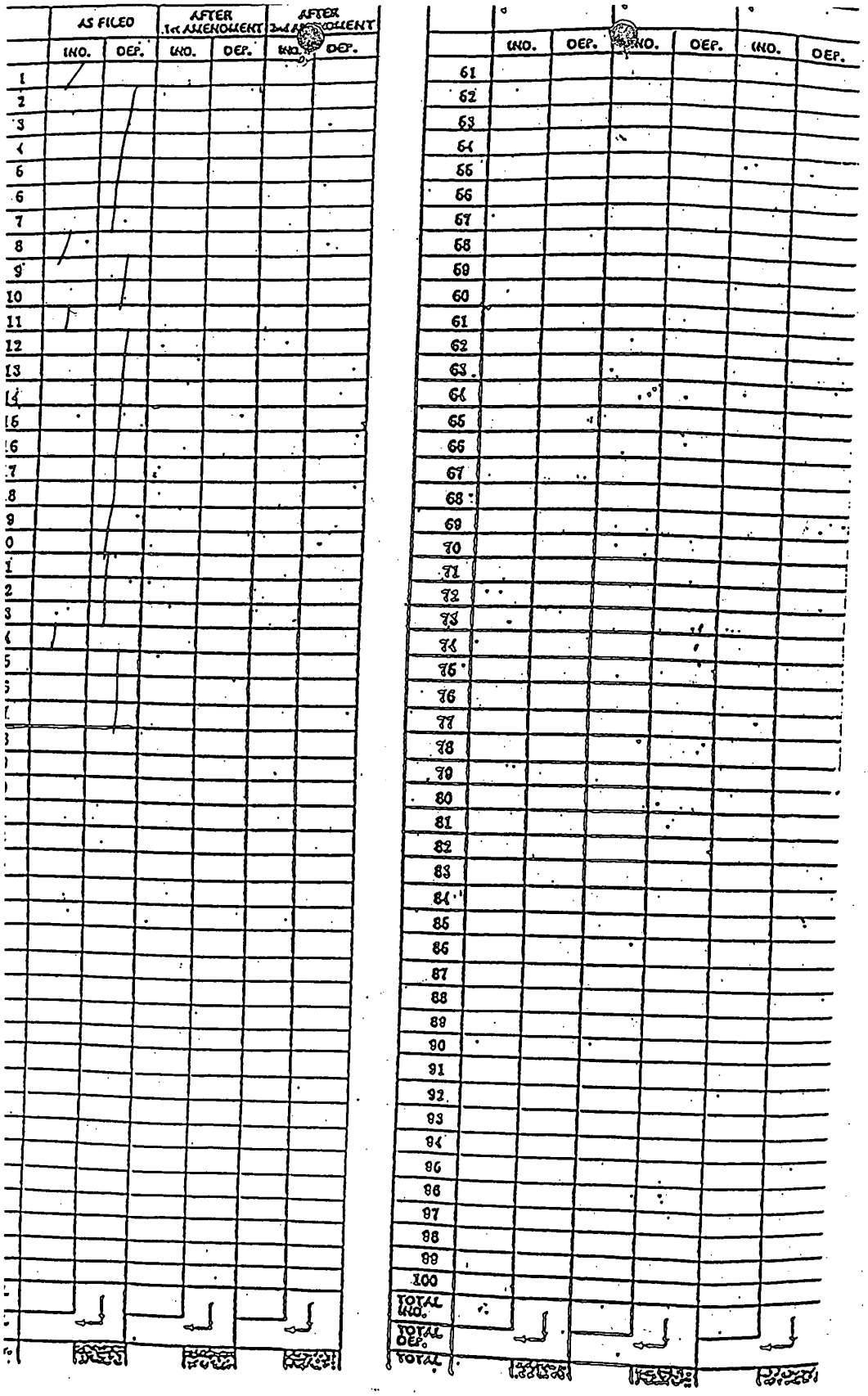
	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X39=		OR	X78=	
+130=		OR	+260=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
***If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

FORM PTO-875
(Rev. 12/99)

Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
*U.S. GPO: 2000-463-433/28044


AS FILED
AFTER 1st ASSESSMENT
AFTER 2nd ASSESSMENT
NO.
DEP.
TOTAL NO.
TOTAL DEP.
TOTAL

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Sten-Olov Engberg, et al.	Group Art Unit Unknown
App. No.	:	Unknown	
Filed	:	Herewith	
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION	
Examiner	:	Unknown	



INFORMATION DISCLOSURE STATEMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed is form PTO-1449 listing references that are also enclosed. This Information Disclosure Statement is being filed within three months of the filing date of this application, and no fee is required in accordance with 37 C.F.R. § 1.97(b)(1).

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: MARCH 6, 2000

By: Jerry T. Sewell

Jerry T. Sewell
Registration No. 31,567
Attorney of Record
620 Newport Center Drive
Sixteenth Floor
Newport Beach, CA 92660
(949) 760-0404

JTS-4504.DOC:ke
20000303

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. APRILS.001A	APPLICATION NO. Unknown
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	APPLICANTS Sten-Olov Engberg, et al.	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE Herewith	GROUP Unknown

jc530 U.S. PTO 09/519829 03/06/00

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPROPRIATE)

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
MH 12/3/03		*Security Dynamics-SecurID Tokens Datasheet,* http://www.computerterps.com/internet/security/secdyn/tokens.html., last modified 7/31/98.
MH 12/3/03		*ACE/Server,* http://www.computerps.com/internet/security/secdyn/aceserv.html, last modified 7/15/98.
MH 12/3/03		*RSA Security Inc.-RSA SecurID Two-Factor Authenication System,* http://www.securid.com/products/securid/index.html., printed on 3/3/00.

JTS-4505.DOC:ke20000306

EXAMINER MH	DATE CONSIDERED 12/3/03

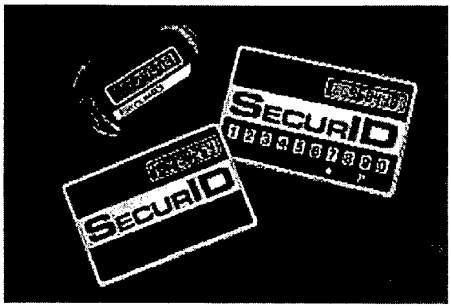
*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

Authentication Tokens

Easy, One-step Process for User Authentication

The SecurID token provides an easy, one step process to positively identify network and system users and prevent unauthorized access. Used in conjunction with Security Dynamics' hardware or software access control modules (ACMs), including ACE/Server, the SecurID token generates a new, unpredictable access code every 60 seconds. SecurID technology offers crackproof security for a wide range of platforms in one easy-to-use package.

Highlights



- Easy, one-step process for positive user authentication
- Prevents unauthorized access to information resources
- Authenticates users at network, system, application or transaction level
- Generates unpredictable, one-time-only access codes that automatically change every 60 seconds
- No token reader required; can be used from any terminal, PC, laptop or workstation - ideal for remote access
- Works across ACMs for multiple platform enterprise security
- Lifetime warranty
- Tamperproof

The SECURID Solution

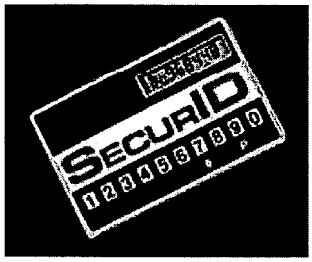
For a sophisticated hacker or a determined insider, it doesn't take much to compromise a user's password and gain access to confidential resources. And when an unauthorized user enters a supposedly secure system all privilege definition and audit trail functions become virtually meaningless . . . in essence, the damage is done. Single-factor identification - a reusable password - is not enough.

To identify and authenticate an authorized system user, two factors are necessary. Factor one is something secret only the user knows: a memorized personal identification number (PIN) or password. The second factor is something unique the user possesses: the SecurID token.

Carried by authorized system users, SecurID tokens - available in three models - generate unique, one-time, unpredictable access codes every 60 seconds. To gain access to a protected resource, a user simply enters his or her secret PIN, followed by the current code displayed on the SecurID token. Authentication is assured when the ACM recognizes the token's unique

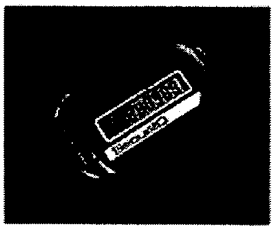
code in combination with the user's unique PIN. Patented technology synchronizes each token with a hardware or software ACM. The ACM may reside at a host, operating system, network/client resource or communications device - virtually any information resource that needs security.

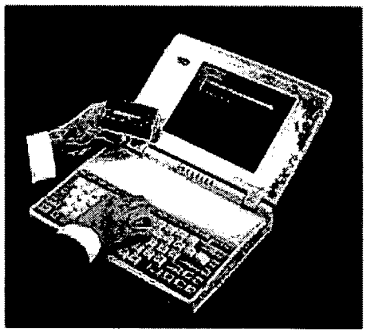
This simple, one-step login results in crackproof computer security - security that's easy to use and administer. The tokens require no card readers or time-consuming challenge/response procedures. With SecurID tokens, reusable passwords can no longer be compromised. Most importantly, access control remains in the hands of management.



SECURID PINPAD[tm] tokens enhance access security
An added level of security can be implemented with a SecurID PINPAD token. The PINPAD token enables users accessing the network to login with an encrypted combination of the PIN and SecurID token code. Using the keypad on the face of the PINPAD token, a user enters his or her secret PIN directly into the token, which generates an encrypted PASSCODETM. This additional level of security is especially appropriate for users in application environments who are concerned that a secret PIN might be compromised through electronic eavesdropping.

SECURID key fob is ideal for any environment
The compact size and durability of the SecurID key fob offer a new dimension in convenience to those customers requiring high levels of security in multiple environments. In addition to providing the same reliable performance in generating random access codes as the original SecurID token, the SecurID key fob comes in a small, light-weight format.





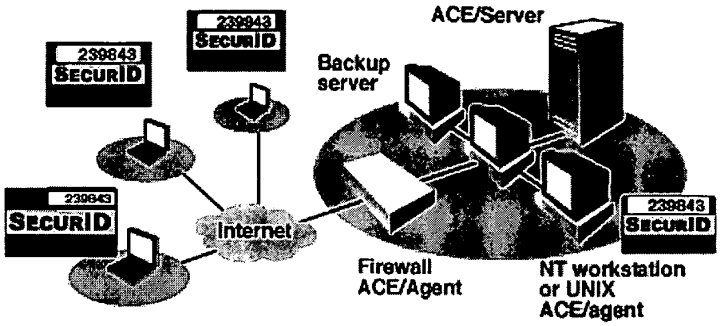
Work with all Security Dynamics access control products
SecurID tokens work in conjunction with all of Security Dynamics' access control products. Hardware and software ACMs offer host-based mainframe security for virtually any platform. ACE/Server network security software operates on a variety of UNIX platforms, establishing a protective perimeter around select network resources. A single SecurID token may be used on multiple ACMs.

SecurID tokens are used with ACMs to solve real security problems: protecting dial-up access lines, securing hosts and/or applications, controlling network access via gateways and securing LANs and TCP/IP and TACACS networks. Millions of of SecurID tokens have been distributed to users worldwide in major businesses, industry, government and academic environments.

Netsite: http://www.computerps.com/internet/security/secdyn/tokens.html
File MIME Type: text/html
Source: Currently in disk cache
Local cache file: MVJAGR2N.HTM
Last Modified: Thursday, July 30, 1998 7:07:09 PM Local time
Last Modified: Friday, July 31, 1998 2:07:09 AM GMT
Content Length: 6945
Expires: No date given
Charset: iso-8859-1
Security: This is an insecure document that is not encrypted and offers no security protection.

ACE/Server

Powerful, Easy-to-Manage Security for your Enterprise Network



Overview

If you think managing security policies across your enterprise network has to be complex and difficult, think again. With ACE/Server from Security Dynamics, you can create a virtually impenetrable barrier against unwanted access to your vital information assets. And all you do is point and click.

ACE/Server works in conjunction with our patented SecurID token and ACE/AgentTM software, providing strong two-factor authentication that verifies the identity and legitimacy of all users attempting to login to your network. Best of all, ACE/Server is compatible with most remote access and network vendor products, so it fits right into your existing management structure.

Highlights

- **Cost-effective network security with industry-leading performance and scalability**
- **Easy to use administrative and audit features**
- **Compatible with all major network hardware and software products**
- **User and administrator auditing with full reporting**
- **Centralized management of user passwords**
- **Built-in support for mobile users**
- **Emergency access features**
- **Support for multiple tokens per user**
- **Operates on a wide range of UNIX-based platforms and Windows NT**

ACE/Server establishes a virtually impenetrable barrier around network resources.

Solid protection of your enterprise network

ACE/Server lets you create a secure perimeter around selected network-based resources. It provides central authentication for all access points--direct-dial communications servers, Internet firewalls, network routers, applications, etc. Our patented time-based security algorithm and two-factor authentication system ensure that only authorized users can login to your network.

You simply point and click to set up users and specify access parameters--keeping administration time and costs to a minimum. As your security needs change,

ACE/Server offers extensive performance and scalability to grow with your organization--supporting a widely distributed, enterprise-wide user population. Customizable auditing and reporting capabilities uncover any attempts to penetrate your secure environment.

With ACE/Server enterprise security, mobile users can access network resources from any geographic location without the need to carry multiple security tokens or remember different user IDs, Passwords, PINs, or server names. By allowing user information to be shared among regional servers, the ACE/Server system enables a business traveler to access the network from, say, London using the same login procedures as in New York. Should a user lose the SecurID token, ACE/Server's emergency access feature lets the administrator issue a unique, one-time-only password or set a temporary passcode.

For the security assurance you need, with the performance and ease-of-use to support diverse user demands, ACE/Server is the foundation for supporting your entire enterprise network.

ACE/Server makes managing your security environment simple and straightforward. It provides a point-and-click interface to set up users, assign or delete tokens, and define access parameters. You can also categorize users into groups for fast, accurate management of user privileges.

Industry-leading performance and scalability

ACE/Server features a robust relational database that scales in size and performance to meet your enterprise security needs, supporting multiple points of administration across your distributed network. All records are indexed for simple, quick retrieval from the database. With ACE/Server you get tremendous flexibility plus the highest degree of scalability and performance in the information security marketplace.

Extensive reporting

With ACE/Server you have extensive custom auditing and reporting capabilities. You can view and report on events using the features most relevant to your security requirements.

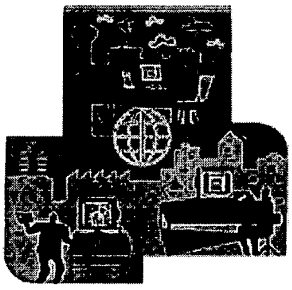
Maximum server availability

To maximize the availability of your authentication services, ACE/Server supports a hot backup to the primary server. This affords you an extra level of confidence that even in the event of hardware or network failure, you will have reliable, secure access for your end users.

Netsite: http://www.computerps.com/internet/security/secdyn/aceserv.html
File MIME Type: text/html
Source: Currently in disk cache
Local cache file: MUCS59RK.HTM
Last Modified: Friday, July 31, 1998 7:16:44 PM Local time
Last Modified: Saturday, August 01, 1998 2:16:44 AM GMT
Content Length: 5148
Expires: Wednesday, July 15, 1998 1:00:00 AM
Charset: iso-8859-1
Security: This is an insecure document that is not encrypted and offers no security protection.

RSA SecurID

Securing Your Future with Strong Authentication



Find information on a product! Go!

Do you really know who's accessing your most sensitive networked information assets? Unfortunately, security built on static, reusable passwords has proven easy for hackers to beat. With the advent of e-business, the need for rock-solid user authentication has never been more urgent.

RSA SecurID two-factor Authentication is based on something you *know* (a password or PIN), and something you *have* (an authenticator) -- providing a much more reliable level of user authentication than reusable passwords.

"Performance and scalability are critical to our customers' operations, and RSA Security has come through again with a winner."

Jason Comstock
Director, Authentication and Information Security
UUNET, an MCI WorldCom company

MCI WORLDCOM

- Free RSA SecurID Token Trial [Downloads]
- RSA Conference 2000 Expands to Europe [Conference]

- For a free RSA SecurID Trial, click now!

Important RSA SecurID Life-cycle News

- New List of Supported Versions Effective 1/1/2000

SC INFOSECURITY MAGAZINE

SC Magazine Names RSA SecurID and RSA ACE/Server 4.0 "Best Buy" for Authentication Solutions

The RSA SecurID Two-Factor Authentication System

- RSA SecurID Authenticators
- RSA ACE/Server
- **New!** RSA ACE/Agents
- RSA SecurID Express

NETWORK COMPUTING EDITOR'S CHOICE

RSA SecurID Success Stories

- Beth Israel Deaconess Medical Center
- NTT PC Communications
- CIBA Specialty Chemicals
- Credit Suisse
- Lufthansa Crew Remote Access

Faster, Easier Security

- **Fast:** Introducing High Performance RSA ACE/Server 4
- **Easy:** The All New SecurID Express
- **Interoperable:** Featuring Dozens of RSA SecurID Partners

---

Our Customers are Using RSA SecurID Today to Protect

- Remote Access
- Enterprise Networks
- e-Business

United States: 1-877-RSA-4900 or 781 301 5000, Europe, Middle East, Africa: +44 118 936 2600,
Asia/Pacific: +65 733 5400, Japan: +81 3 3539 7667

Location: http://www.securid.com/products/securid/index.html
File MIME Type: text/html
Source: Currently in disk cache
Local cache file: MUN97F98.HTM
Last Modified: Unknown
Last Modified: Unknown
Content Length: 32372
Expires: No date given
Charset: Unknown
Security: This is an insecure document that is not encrypted and offers no security protection.

FORMALITIES LETTER

OC000000005051458

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENT AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NUMBER	FILING/RECEIPT DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
09/519,829	03/06/2000	sTEN-Olov Engberg	APRILS.001A

20995
KNOBBE MARTENS OLSON & BEAR LLP
620 NEWPORT CENTER DRIVE
SIXTEENTH FLOOR
NEWPORT BEACH, CA 92660

Date Mailed: 04/14/2000

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given TWO MONTHS from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
  Applicant must submit **$ 690** *to complete the basic filing fee and/or file a small entity statement claiming such status (37 CFR 1.27).*
- Total additional claim fee(s) for this application is $204.
  - **$126** for **7** total claims over 20.
  - **$78** for **1** independent claims over 3 .
- The oath or declaration is missing.
  A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(e) of $130 for a non-small entity, must be submitted with the missing items identified in this letter.
- **The balance due by applicant is $ 1024.**

A copy of this notice MUST be returned with the reply.

Janice Bruce

Customer Service Center
Initial Patent Examination Division (703) 308-1202

PART 3 - OFFICE COPY

OIPE
MAY 2 3 2000
PATENT & TRADEMARK OFFICE

APRILS.001A

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED
MAY 25 2000
TECH CENTER 2700

Applicants	:	Engberg, et al.	Group Art Unit 2777
App. No.	:	09/519,829	
Filed	:	March 6, 2000	
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION	
Examiner	:	UNKNOWN	

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed is form PTO-1449 listing three (3) references that are also enclosed. This Supplemental Information Disclosure Statement is being filed before the receipt of a first Office Action on the merits, and presumably no fee is required in accordance with 37 C.F.R. § 1.97(b)(3). If a first Office Action on the merits was mailed before the mailing date of this Statement, the Commissioner is authorized to charge the fee set forth in 37 C.F.R. § 1.17(p) to Deposit Account 11-1410. A duplicate copy of this Statement is enclosed for that purpose.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: May 19 2000

By: _____

Alexander Franco
Registration No. 45,753
Attorney of Record
620 Newport Center Drive, Sixteenth Floor
Newport Beach, CA 92660
(949) 760-0404

H:\DOCS\ASF\ASF-1434.DOC
051900

OIPE
MAY 2 3 2000
PATENT & TRADEMARK OFFICE

PATENT

Gp 2777

Case Docket No. APRILS.001A
Date: May 19, 2000

RECEIVED
MAY 25 2000
TECH CENTER 2700

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Engberg, et al.
Appl. No.	:	09/519,829
Filed	:	March 6, 2000
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
Examiner	:	UNKNOWN
Group Art Unit	:	2777

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on

May 19, 2000
(Date)

Alexander Franco, Reg. No. 45,753

TRANSMITTAL LETTER

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

ATTENTION: APPLICATION BRANCH

Dear Sir:

Enclosed for filing in the above-identified application are the following documents:

(X) A Supplemental Information Disclosure Statement;

(X) A PTO Form 1449 listing three (3) references, copies of which are enclosed; and

(X) A return prepaid postcard.

The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment, to Account No. 11-1410. A duplicate copy of this sheet is enclosed.

Alexander Franco
Registration No. 45,753
Attorney of Record

H:\DOCS\ASF\ASF-1436.DOC\dns
051900

KNOBBE, MARTENS, OLSON & BEAR, LLP
620 NEWPORT CENTER DR 16TH FLOOR NEWPORT BEACH, CA 92660
(949) 760-0404 FAX (949) 760-9502

Security Scanning & Penetration | Security Engineering & Auditing | Security Workshops | Security Products

monkey (mobile network key)

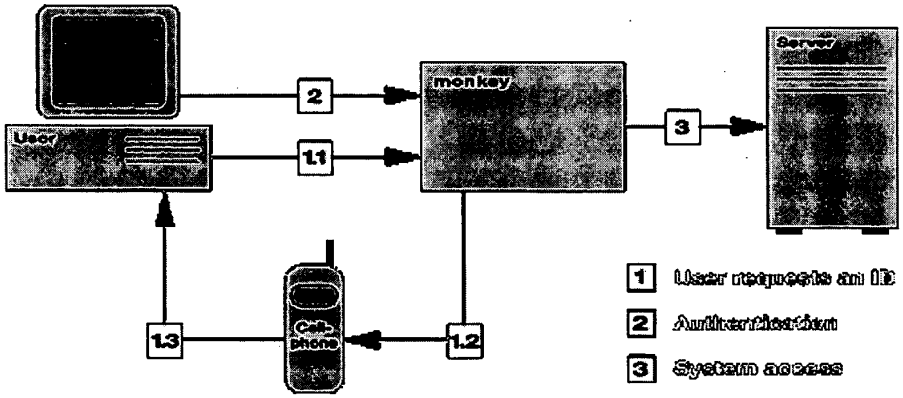
24-hour cellphone cyberwatch

monkey (mobile network key) is the first security solution of its kind. Developed by data protect, it offers simple, yet highly effective, protection against unauthorized access to your data.

monkey is based on a two-step authentication system. The user requests a password using his or her GSM cellphone, which acts as the hardware token. The authentication server generates a cryptographic one-off password and transmits this to the user's GSM network.

The user then has a limited period of time (e.g. 2 minutes) to log on to the monkey-protected server using this password. thanks to the limited validity of this password (it must be used during the session in which it was requested), monkey clearly surpasses the level of security offered by standard time-based tokens.

monkey can be deployed across a broad spectrum of applications, ranging from the internet and intranets to non-computer-related authentication scenarios, such as online shopping, online banking and micro payments.

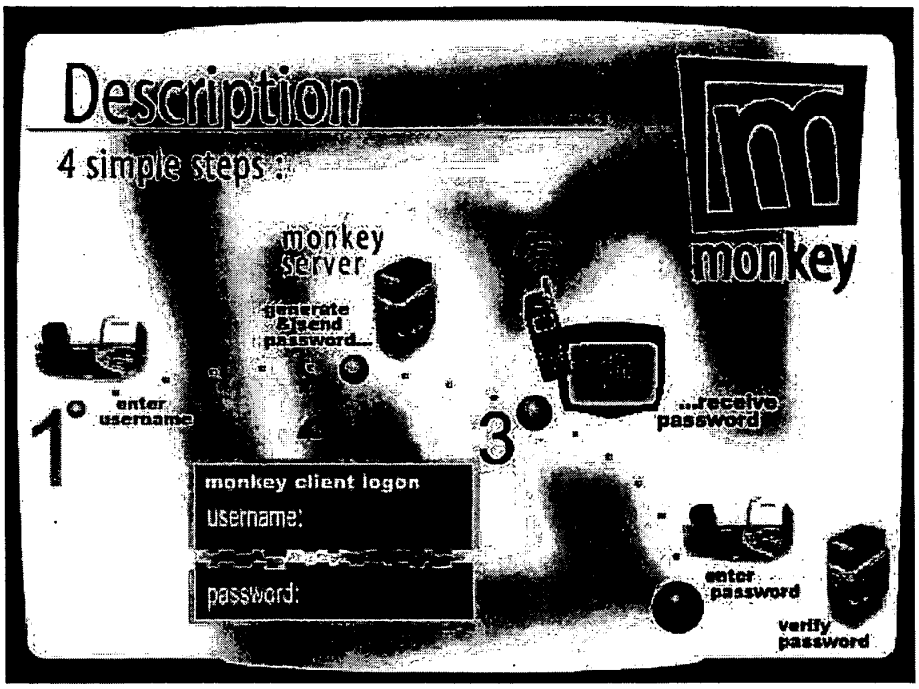


monkey as authentication software

monkey (mobile network key) is a data security software solution. It was originally developed as a pure authentication system with the goal of simply and effectively blocking unauthorized access to data.

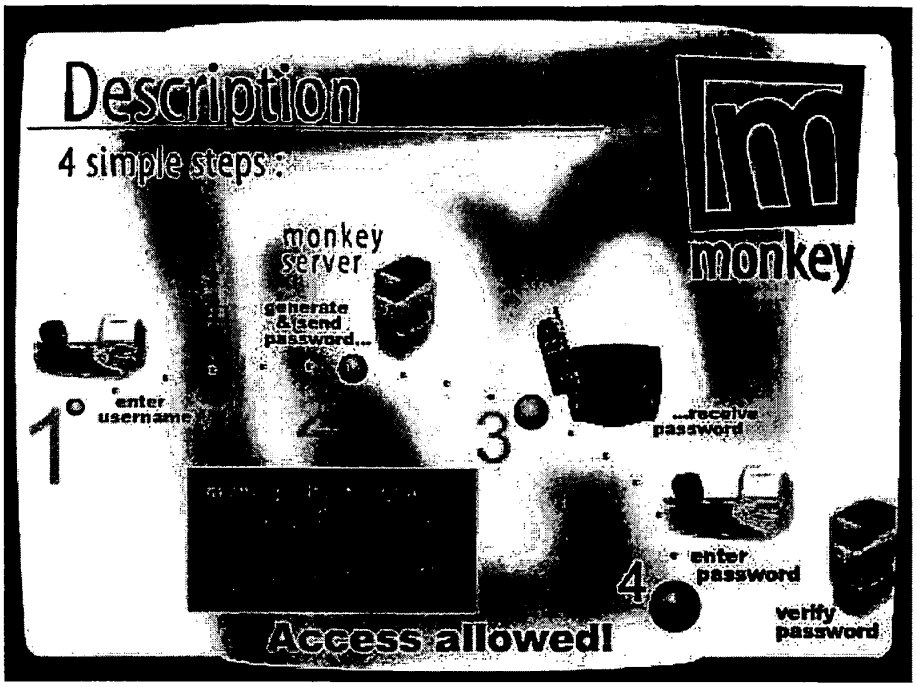
However, monkey can also be used as a payment method for internet shopping. In order to demonstrate the functionality of this product, we will show monkey as an authentication system.

The patent for the underlying process was applied for in 1997.



In order to get access to a server which is protected by monkey, a user first logs in with his name (step 1). The monkey server then generates a random one-time password and transmits it to the user's mobile phone (step 2 and 3). This one-time password is transmitted as a SMS message to the user's phone within 5 seconds.

After receiving this password on his/her mobile telephone, the user has to enter it into his/her computer within 2 minutes. The monkey server compares the user provided password with the generated password and grants access to the system if they are equivalent (step 4). The password is bound to the session such that it becomes invalid immediately after a successful login. This eliminates the possibility of a replay attack.



The following conditions would have to be met for a successful attack:

- the user's GSM card is stolen,
- the appropriate PIN code is known,
- the user identification is known,
- and if required, the fixed password for the relevant server is known.

monkey has the following benefits:

- monkey uses an existing infrastructure (GSM network and mobile telephones), thus no additional hardware is necessary.
- monkey is independent of operating systems.
- monkey integrates easily in existing security systems (radius protocol).
- The user only has to remember the PIN of the mobile telephone. For additional security, the user can be required to enter this PIN in addition to the monkey SMS code.

Application areas of monkey include:

- local networks,
- internet- / intranet- / extranet-applications,
- e-commerce applications / online-shopping,
- electronic-banking,
- micropayments

monkey (mobile network key)

Technical Overview (draft)
July, 25th 1999



1. Introduction
2. monkey concepts
3. Security
4. Reliability
5. Performance
6. Compatibility
7. monkey implementation
------7a. *User database modules*
------7b. *SMS transmission modules*
------7c. *Authentication modules*
------7d. *Log modules*
8. monkey in electronic commerce and online banking

1. Introduction

The mobile network key ("monkey") is a 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 mobile telephony, and thus turns any GSM mobile telephone into an authentication token. Every GSM telephone is capable of receiving and displaying short messages.

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 her 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.

Speaking more technically, monkey is an authentication server that handles generation, transmission and verification of one-time passwords in response to client requests. In the context of this paper, the term "client" denotes the point of authentication, i.e. an entity that collects a user's credentials, passes them to the authentication server and, according to the server's reply, grants or denies access to the user. |top|

2. monkey concepts

The monkey architecture clings to the maxim "keep it simple", which has resulted in a straightforward and comprehensible server design in hardly more than 10.000 lines of C code. Starting from this maxim, monkey has been conceived and implemented whilst strictly adhering to the paramount design criteria of security, reliability, performance and compatibility. [top]

3. Security

monkey security relies exclusively on methods that are well-known and which have passed extensive academic review, such as the MD5 message digest algorithm. Still, extreme care has been taken to not only use these methods, but to use them in a secure context as well. Even the best cryptographically secure random number generator, for example, is hardly worth anything if it is fed by a seed value that contains merely 40 bits of entropy, which can be compromised by a not-so-brute-force attack - even if the generator is built around algorithms that are "known to be good". Hence, additions to the monkey design and the corresponding source code tree are periodically audited by different persons in order to discover and eliminate even the most subtle variant of this class of problems. In addition, data protect encourages peer review of the source code and the algorithm design by their partners. The simpleness inherent to monkey and the compact implementation in about 10.000 lines of code make this quite a feasible task.

monkey tries to minimize the risk of administrative mistakes as well, such as a poorly chosen seed phrase for the cryptographically strong one-time password generator. It therefore provides a reasonable default configuration, e.g. a random seed created by collecting entropy from various sources, the security of which can only be tightened - and not weakened - by an administrator, e.g. by supplying a pass phrase to add bits to the existing pool of entropy. [top]

4. Reliability

Even the best design will be defeated, if its implementation fails to match the specification. Experience shows that implementation errors are far more commonplace than instances of "broken by design". In addition to the above mentioned source code audits, data protect has therefore established guidelines for writing software that will fail in a controlled way, i.e. log an error message and resume operation - if it fails at all. The guidelines include, among many other rules, sufficient bounds checking to prevent buffer overflow problems, checking the return value of any non-void function and gracefully handling all possible situations, enabling the full set of compiler warnings, or carefully documenting modifications to the CVS source code repository.

The monkey architecture is highly modular and each module executes as a separate process in a separate address space. In addition, interprocess communication (IPC) is restricted to simple messages, the integrity of which can easily be verified by their recipients. Thus, a process that has become unstable, would be strictly confined to its own address space and hence be prevented from affecting the other

processes' operation. Eventually, rigorous testing under heavy load and other typically problematic conditions, such as low memory, is an absolute "must" for any monkey version to be released. |top|

5. Performance

At first glance, reliability appears to be the natural enemy of performance. Extensive parameter checking and the modular structure, which coincides with an enormous number of IPC messages and thus with considerable overhead, seem to make performance penalties inevitable. However, although maintaining the additional security provided by process address space boundaries, monkey manages to dramatically reduce IPC traffic. Consider the case that process A asks process B to do a lookup and return the result. This scenario requires two IPC messages: the message that tells B to perform the lookup and the message in which B returns the result to A. However, if A maintained a copy of B's data, A could do the lookup itself and save two IPC messages. The monkey design makes extensive use of this principle, without sacrificing its modularity: at startup, every process is given an identical local copy of static configuration data, i.e. configuration data that will not change throughout the process's lifetime.

IPC traffic is further reduced by having each process locally cache the results of its previous requests. So, in case of a cache hit, IPC is not necessary at all, since the corresponding result is available in local address space. In addition to reducing the number of messages, IPC overhead can be reduced by minimizing their size. Therefore, monkey IPC messages implement very lightweight protocols, that merely transmit the most essential data. However, the modularity of the monkey architecture is not only a curse regarding performance, it can also be a blessing. Owing to the high degree of parallelism, monkey scales very well on multi-processor machines.

Besides optimizations like these, which aim to optimally implement a given architecture, careful design of the architecture to be implemented is a determining factor concerning overall performance. monkey therefore employs efficient algorithms and data structures, such as balanced binary trees (e.g. AVL trees), which provide inexpensive lookups in logarithmic time, in those parts of the server that are pivotal to its performance. Nevertheless, all algorithms are still kept as simple as possible.

To sum up, running under Linux on a 300 MHz Pentium II based single-CPU system, monkey is able to handle well over 1.000 authentications per second. |top|

6. Compatibility

monkey is typically deployed as part of an overall solution. So it is essential for monkey to smoothly integrate with an existing infrastructure. This implies that the authentication server has to be available on a variety of hardware platforms, in order to cater for the diversity of IT infrastructures (portability) and it must be able to communicate with the surrounding components, e.g. the point of authentication (openness).

monkey is highly portable and therefore currently supports Solaris (Sparc and Intel), HP-UX (HP-PA), standard DG/UX (Intel), the B2 evaluated version of DG/UX (Intel), Linux (Intel and Alpha), the various free BSD variants (Intel) and, requiring about 10 to 50 additional lines of code per

port, probably any POSIX compliant Unix implementation. A port to Windows NT, which seamlessly integrates with the NT paradigm by running as a service, is available as well.

The openness of monkey stems from an absolute commitment to open standards and de facto standards, such as LDAP and RADIUS among the former or SQL among the latter. Moreover, monkey offers a library of C functions that implement monkey client functionality such as requesting or verifying one-time passwords locally or via a network connection. The time spent writing a monkey "shim" for clients that do not support open protocols but a proprietary authentication interface, i.e. middleware that maps the proprietary requests to monkey requests and vice versa, is thus dramatically reduced. In addition, wrapper programs that provide a command line interface to the library functions, such as "reqpw" and "chkpw" to request and verify passwords, are supplied with monkey to simplify their use in CGI-like applications. As of this writing, a Java and a Perl version of the client library are being worked on. |top|

7. monkey implementation

The monkey authentication server consists of four different kinds of modules which are at runtime instantiated as processes. |top|

a. User database modules

These modules handle the mapping from user names to the corresponding mobile phone numbers by performing a lookup in the user database. monkey currently includes user database modules foraccessing database management systems via LDAP, SQL and ODBC (Windows NT only), and for highly efficient indexed flat file user databases. Aiming at compatibility, monkey is designed to integrate with an existing database infrastructure, instead of maintaining a separate dedicated database of monkey users. |top|

b. SMS transmission modules

They are responsible for transmitting a given short message to a specified mobile phone number. The Siemens "M" family of GSM modules, which basically consists of stationary mobile phones that can be attached to the serial interface of a computer, as well as potentially any other GSM module that adheres to the standard for GSM AT commands, are currently supported for low-bandwidth applications, as is UCP via a dedicated X.25 link for a direct high-bandwidth connection to a GSM short message service center. Load balancing to evenly distribute the SMS traffic over several channels in order to increase the total bandwidth available for SMS transfers in high-end scenarios is implemented as well. |top|

c. *Authentication modules*

These modules maintain the link between monkey and the authentication clients. On incoming requests, they generate the one-time passwords, ask the user database modules to find the phone number of the user to be authenticated, form a short message containing the generated password and transmit the short message by passing it to one of the SMS transmission modules. As of this writing, the RADIUS

Internet standard is the authentication protocol employed. For electronic commerce applications an additional proprietary protocol has been developed, which is capable of transferring encrypted billing information to the monkey server. Moreover, a module exists that integrates with the authentication services of the B2 certified version of Data General's DG/UX. |top|

d. Log modules

They are responsible to pass messages received from other modules to a log database. Currently, only flat file logging is supported. However, the log functions are in the process of being heavily restructured to make logging to databases possible in a way that takes optimal advantage of the structure of relational database management systems. |top|

8. monkey in electronic commerce and online banking

We consider monkey to be the safest solution for user authentication in electronic commerce and online banking applications. Competing solutions typically rely on digital signatures, i.e. the customer fills out an online ordering form, his or her ordering form is then digitally signed - either by a chip card plugged into or by security software running on his or her computer - and eventually transmitted to the merchant's electronic commerce server. The integrity of the customer's computer is pivotal to this mechanism. Otherwise the following trivial attack defeats the whole security scheme.

Suppose that Alice is ordering goods from Bob's online shop. However, Eve is the creator of a virus which has infected Alice's computer or, alternatively, of a troyan horse that she tricked Alice into executing. When Alice finishes the ordering form, Eve's malicious code intercepts the form before the digital signature is applied and manipulates it - without Alice noticing - to Eve's advantage, e.g. changes the shipping address to her address. Eve's code then passes the modified ordering form to the signature mechanism where it gets digitally signed. Eventually, an ordering form with Alice's digital signature is passed to Bob.

As can be seen, the security problem arises, because Alice is unable to control what she signs. The same attack applies to online banking, giving Eve the power to redirect money transfers to her own bank account. As viruses tend to spread quickly, Eve has the potential to attack not only Alice but also thousands of other customers and thus to commit large scale fraud.

Other one-time password schemes fall prey to the same attack, since Alice has no means of making sure that the order or the money transfer she confirms by submitting the one-time password has not been modified on its way to Bob. She is able to verify what she has entered. Yet, she is not able to verify whether what she has entered matches what Bob has received.

monkey is resistant against this class of attacks, i.e. monkey does not rely on the integrity of the customer's computer. Judging from the average user and his or her computer, this is what we consider to be the foremost goal that every serious effort to provide security for online transactions must achieve.

Again, suppose that Alice orders goods from Bob's online shop. She fills out the ordering form and submits it to Bob's electronic commerce server. Bob replies with a GSM short message that lists Alice's order (or at least the shipping address) and the monkey one-time password. In other words, Alice is made aware of what exactly she is going to confirm by entering the monkey password and thus becomes able to tell whether the order that Bob received matches the order she transmitted. After verifying the short message, Alice confirms her order by transmitting the monkey password to Bob to prove her identity. So, monkey completely eliminates the need for Alice ensuring the integrity of her computer.

A prototype of an integration with the Intershop electronic commerce software is available at http://194.221.145.77

As of this writing, we are implementing an interface to link monkey servers to the billing infrastructure of GSM service providers. In the near future, Alice will have the option to pay the goods she has purchased via her mobile phone bill. [top]

OIPE JC67
JUN 19 2000
PATENT & TRADEMARK OFFICE

Sceter

PATENT

Case Docket No. APRILS.001A
Date: June 16, 2000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Engberg, et al.
App. No.	:	09/519,829
Filed	:	March 6, 2000
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
Group Art Unit	:	2777

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on

June 16, 2000
(Date)

Alexander Franco, Reg. No. 45,753

TRANSMITTAL LETTER

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

ATTENTION: BOX MISSING PARTS

Dear Sir:

In response to the Notice to File Missing Parts of Application Under 37 CFR 1.53(f), which was mailed by the Office on April 14, 2000, enclosed are the following documents:

(X) An executed Declaration by Inventor(s);

(X) A Power of Attorney Form and Copy of Assignment;

(X) A verified statement to establish small entity status under 37 CFR 1.9 and 1.27;

(X) A Notice to File Missing Parts;

(X) An extension of time to respond for 1 month is hereby requested;

(X) A check in the amount of $669.00 to cover the fees; and

(X) A return prepaid postcard.

06/21/2000 TTRAN1 00000090 09519829
55.00 OP
06 FC:215

KNOBBE, MARTENS, OLSON & BEAR, LLP
620 NEWPORT CENTER DR 16TH FLOOR NEWPORT BEACH, CA 92660
(949) 760-0404 FAX (949) 760-9502

Fees as calculated below:

Time Extension Fee:

(X)	one month	($55 small entity)
()	two months	($190 small entity)
()	three months	($435 small entity)

FILING FEE UNPAID AT TIME OF FILING		$ 549.00
FEE FOR EXTENSION OF TIME (SMALL ENTITY)	1 month	$ 55.00
SURCHARGE 37 CFR 1.16(e)		$ + 65.00
TOTAL FEES SUBMITTED HEREWITH		$ 669.00

The Commissioner is hereby authorized to charge any additional fees which may be required, now or in the future, or credit any overpayment, to Account No. 11-1410. A duplicate copy of this sheet is enclosed.



Alexander Franco
Registration No. 45,753
Attorney of Record

H:\DOCS\ROS\ROS-2190.DOC\dns
061600

03CO

FORMALITIES LETTER

OC000000005051458

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENT AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NUMBER	FILING/RECEIPT DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
09/519,829	03/06/2000	sTEN-Olov Engberg	APRILS.001A

20995
KNOBBE MARTENS OLSON & BEAR LLP
620 NEWPORT CENTER DRIVE
SIXTEENTH FLOOR
NEWPORT BEACH, CA 92660

OIPE JC67 JUN 19 2000 PATENT & TRADEMARK OFFICE

Date Mailed: 04/14/2000

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given TWO MONTHS from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
  Applicant must submit **$ 690** *to complete the basic filing fee and/or file a small entity statement claiming such status (37 CFR 1.27).*
- Total additional claim fee(s) for this application is $204.
  - **$126** for **7** total claims over 20.
  - **$78** for **1** independent claims over 3 .
- The oath or declaration is missing.
  A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(e) of $130 for a non-small entity, must be submitted with the missing items identified in this letter.
- **The balance due by applicant is $ 1024.**

*A copy of this notice **MUST** be returned with the reply.*

Janice Louse

Customer Service Center
Initial Patent Examination Division (703) 308-1202
PART 2 - COPY TO BE RETURNED WITH RESPONSE

06/21/2000 TTRAN1 00000090 09519829
01 FC:201 345.00 OP
02 FC:202 39.00 OP
03 FC:203 63.00 OP
04 FC:205 65.00 OP
05 FC:299 102.00 OP

OIPE JC67 JUN 19 2000 PATENT & TRADEMARK OFFICE

DECLARATION - USA PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION; the specification of which was filed on **March 6, 2000** as Application Serial No. **09/519,829**.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above;

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56;

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 validity of the application or any patent issued thereon.

Full name of first inventor: **Sten-Olov Engberg**

Inventor's signature _____

Date May 11 2000

Residence: **Sanglarkvagen 5, S-743 30, Storvreta, Sweden**

Citizenship: **Sweden**

Post Office Address: **Same As Above**

Full name of second inventor: **Ake Jonsson**

Inventor's signature Ake Jonsson

Date May 11 2000

Residence: **Linjan 4, S-737 40, Fagersta, Sweden**

Citizenship: **Sweden**

Post Office Address: **Same As Above**

Send Correspondence To:
KNOBBE, MARTENS, OLSON & BEAR, LLP
Customer No. 20,995

H:\DOCS\ASF\ASF-1427.DOC\dns
051000

OIPE JUN 19 2000 PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Engberg, et al.
App. No.	:	09/519,829
Filed	:	March 6, 2000
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
Examiner	:	UNKNOWN

ESTABLISHMENT OF RIGHT OF ASSIGNEE TO TAKE ACTION
AND
REVOCATION AND POWER OF ATTORNEY

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

The undersigned is empowered to act on behalf of the assignee below (the "Assignee"). A true copy of the original Assignment of the above-captioned application from the inventor(s) to the Assignee is attached hereto. This Assignment represents the entire chain of title of this invention from the Inventor(s) to the Assignee.

I declare that all statements made herein are true, and that all statements made upon 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 18 U.S.C. § 1001, and that willful, false statements may jeopardize the validity of the application, or any patent issuing thereon.

The undersigned hereby revokes any previous powers of attorney in the subject application, and hereby appoints the registrants of Knobbe, Martens, Olson & Bear, LLP, 620 Newport Center Drive, Sixteenth Floor, Newport Beach, California 92660, Telephone (949) 760-0404, **Customer No. 20,995**, as its attorneys with full power of substitution and

revocation to prosecute this application and to transact all business in the U.S. Patent and Trademark Office connected herewith. This appointment is to be to the exclusion of the inventor(s) and his attorney(s) in accordance with the provisions of 37 C.F.R. § 3.71.

Please use **Customer No. 20,995** for all communications.

APRIL SYSTEM DESIGN AB

Dated: may 11 2000

By: _____
Sten-Olov Engberg

Title: President

Address: Vretenvagen 2, S-171 54
Solna, Sweden

H:\DOCS\ASF\ASF-1429.DOC\dns
051000

COPY

PTO JC67 JUN 19 2000 PATENT & TRADEMARK OFFICE

ASSIGNMENT

WHEREAS, We, Sten-Olov Engberg, a citizen of Sweden, residing at Sanglarkvagen 5, S-743 30, Storvreta, Sweden and Ake Jonsson, a citizen of Sweden, residing at Linjan 4, S-737 40, Fagersta, Sweden, have invented certain new and useful improvements in a USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION for which we have filed an application for Letters Patent in the United States, which was filed on March 6, 2000 as Application Serial No. 09/519,829;

AND WHEREAS, April System Design, AB (hereinafter "ASSIGNEE"), a Sweden Corporation, with its principal place of business at Vretenvagen 2, S-171 54, Solna, Sweden, desires to acquire the entire right, title, and interest in and to the said improvements and the said Application:

NOW, THEREFORE, in consideration of the sum of One Dollar ($1.00) to me in hand paid, and other good and valuable consideration, the receipt of which is hereby acknowledged, we, the said inventors, do hereby acknowledge that we have sold, assigned, transferred and set over, and by these presents do hereby sell, assign, transfer and set over, unto the said ASSIGNEE, its successors, legal representatives and assigns, the entire right, title, and interest throughout the world in, to and under the said improvements, and the said application and all divisions, renewals and continuations thereof, and all Letters Patent of the United States which may be granted thereon and all reissues and extensions thereof, and all rights of priority under International Conventions and applications for Letters Patent which may hereafter be filed for said improvements in any country or countries foreign to the United States, and all Letters Patent which may be granted for said improvements in any country or countries foreign to the United States and all extensions, renewals and reissues thereof; and we hereby authorize and request the Commissioner of Patents of the United States, and any Official of any country or countries foreign to the United States, whose duty it is to issue patents on applications as aforesaid, to issue all Letters Patent for said improvements to the said ASSIGNEE, its successors, legal representatives and assigns, in accordance with the terms of this instrument.

AND WE HEREBY covenant and agree that we will communicate to the said ASSIGNEE, successors, legal representatives and assigns, any facts known to us respecting said improvements, and testify in any legal proceeding, sign all lawful papers, execute all divisional, continuing and reissue applications, make all rightful oaths and generally do everything possible to aid the said ASSIGNEE, its successors, legal representatives and assigns, to obtain and enforce proper patent protection for said improvements in all countries.

IN TESTIMONY WHEREOF, I hereunto set my hand and seal this 11 day of May, 20 00

COPY

Sten-Olov Engberg

STATE OF

COUNTY OF] ss.

On _____, before me, _____, personally appeared Sten-Olov Engberg personally known to me (or proved to me on the basis of satisfactory evidence) to be the person(s) whose name(s) is/are subscribed to the within instrument, and acknowledged to me that he executed the same in his authorized capacity(ies), and that by his signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

WITNESS my hand and official seal.

[SEAL]

_____
Notary Signature

COPY

IN TESTIMONY WHEREOF, I hereunto set my hand and seal this 11 day of May, 2000

COPY

Ake Jonsson

STATE OF

COUNTY OF ss.

On _____, before me, _____, personally appeared Ake Jonsson personally known to me (or proved to me on the basis of satisfactory evidence) to be the person(s) whose name(s) is/are subscribed to the within instrument, and acknowledged to me that he executed the same in his authorized capacity(ies), and that by his signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

WITNESS my hand and official seal.

[SEAL]

_____
Notary Signature

H:\DOCS\ASF\ASF-1428.DOC\dns
051000

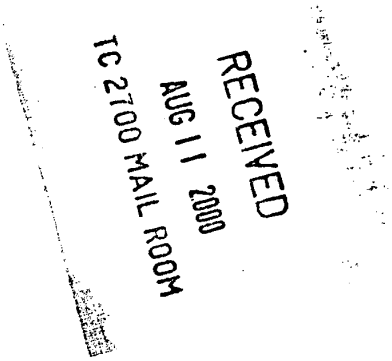


#8 / Prior Art
T. McBeth Brown
2/15/01

APRILS.001A PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Engberg, et al.	Group Art Unit 2777
App. No.	:	09/519,829	
Filed	:	March 6, 2000	
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION	
Examiner	:	UNKNOWN	



INFORMATION DISCLOSURE STATEMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed is form PTO-1449 listing two (2) references that are also enclosed. This Information Disclosure Statement is being filed before the receipt of a first Office Action on the merits, and presumably no fee is required in accordance with 37 C.F.R. § 1.97(b)(3). If a first Office Action on the merits was mailed before the mailing date of this Statement, the Commissioner is authorized to charge the fee set forth in 37 C.F.R. § 1.17(p) to Deposit Account 11-1410. A duplicate copy of this Statement is enclosed for that purpose.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 8/02/00

By: _____

Alexander Franco
Registration No. 45,753
Attorney of Record
620 Newport Center Drive, Sixteenth Floor
Newport Beach, CA 92660
(949) 760-0404

H:\DOCS\ASF\ASF-1529.DOC\dns
080200

OIPE JC93 AUG 0 8 2000 PATENT & TRADEMARK OFFICE

GAU 2777

PATENT

Case Docket No. APRILS.001A
Date: August 2, 2000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Engberg, et al.
Appl. No.	:	09/519,829
Filed	:	March 6, 2000
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
Examiner	:	UNKNOWN
Group Art Unit	:	2777

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on

August 2, 2000
(Date)

Alexander Franco, Reg. No. 45,753

RECEIVED AUG 11 2000 TC 2700 MAIL ROOM

TRANSMITTAL LETTER

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

ATTENTION: APPLICATION BRANCH

Dear Sir:

Enclosed for filing in the above-identified application are the following:

(X) An Information Disclosure Statement;

(X) A PTO Form 1449 listing two (2) references, copies of which are enclosed; and

(X) A return prepaid postcard.

The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment, to Account No. 11-1410. A duplicate copy of this sheet is enclosed.

Alexander Franco
Registration No. 45,753
Attorney of Record

H:\DOCS\ASF\ASF-1530.DOC\dns
080200

KNOBBE, MARTENS, OLSON & BEAR, LLP
620 NEWPORT CENTER DR 16TH FLOOR NEWPORT BEACH, CA 92660
(949) 760-0404 FAX (949) 760-9502

AU9863545

(12) PATENT ABSTRACT (11) Document No. AU-A-63545/98
(19) AUSTRALIAN PATENT OFFICE

(54) Title
METHOD FOR THE AUTHORIZATION IN DATA COMMUNICATION SYSTEMS

(51)[6] International Patent Classification(s)
H04L 009/32

(21) Application No. : **63545/98** (22) Application Date : **22/04/98**

(30) Priority Data

(31) Number	(32) Date	(33) Country
19718103	**29/04/97**	**DE GERMANY**

(43) Publication Date : **05/11/98**

(71) Applicant(s)
KIM SCHMITZ

(72) Inventor(s)
KIM SCHMITZ

(74) Attorney or Agent
GRIFFITH HACK , GPO Box 4164, SYDNEY NSW 2001

(57)

The invention relates to a method and to a device for the authorization in data transmission systems employing a transaction authorization number (TAN) or a comparable password. According to a first step, the user sends a qualifying identification of the data input apparatus together with a request for the generation or for the selection of a transaction authorization number TAN or of comparable password from a data file from the data input apparatus to an authorization computer. In a second step the authorization computer generates the transaction authorization number TAN or the comparable password or selects them form a data file. According to a third step, the authorization computer sends the transaction authorization number TAN or the comparable password over a second transmission path different from the first transmission path to a monitor, for example a handy or a pager. According to a fourth step, the user reads this transaction authorization number TAN or the comparable password from the receiver and enters the transaction authorization number TAN or the comparable password into the data input apparatus. According to a fifth step, this transaction authorization number TAN

.../2

or the comparable password is transmitted to the authorization computer. According to a sixth step, the authorization computer verifies the validity of the transaction-authorization number TAN or of the comparable password in order to establish or switch free, according to a seventh step, a connection between the data input apparatus and the receiver unit.

P/00/011
Regulation 3.2

AUSTRALIA
Patents Act 1990

ORIGINAL

COMPLETE SPECIFICATION

STANDARD PATENT

Invention Title: METHOD FOR THE AUTHORIZATION IN DATA COMMUNICATION SYSTEMS

The following statement is a full description of this invention, including the best method of performing it known to me:

GH REF: P25659-A:MHK:RK

METHOD POR AUTHORIZING IN DATA TRANSMISSION SYSTEMS

BACKGROUND OF THE INVENTION

1. Field of the Invention

The invention relates to a method for authorizing in data transmission and communication systems.

2. Brief Description of the Background of the Invention including Prior Art

It is known that in telebanking or in remote terminal banking the user requires in addition to his or her permanent password (personal identification number PIN) for each individual transaction additionally a transaction authorization number (TAN). Such transaction authorization numbers TANs are transmitted to the user in larger blocks by mail. Thus, there exists the risk that third persons receive knowledge of such transaction authorization numbers TANs and can perform a misuse in connection with the password. The risk is increased by such transaction authorization numbers TANs having a validity which is de facto unlimited in time.

Furthermore, call-back systems are known, wherein the called-in system assures based on a call-back at the generally stored telephone number that the calling system is authorized and that no foreign system pretends to be an authorized system. The disadvantage of the call-back systems comprises that an unauthorized user, who has procured a functional access to the authorized calling system from any possible source, can work without a problem based on this illegally obtained authorization, since the call-back system checks only whether the call-back system has been called by a system which is authorized in principle by a basically authorized system.

Summary of the Invention

At least preferred embodiments of the present invention furnish a method for authorizing and an authorization process in connection with data transmission and data communication, wherein the security of the transmission or communication is increased.

Brief Description of the Invention

In accordance with a first aspect of the present invention there is provided a method for the authorization of data transmission systems. A qualifying identification of a user is entered into a data input apparatus. The qualifying identification and a request for an authorization signal is transmitted from the data input apparatus to an authorization computer along a first transmission path. The authorization signal is established in the authorization computer. The authorization signal is sent from the authori-zation computer to a monitor along a second transmission path different as compared to the first transmission path. The authorization signal at the monitor is read by the user. The authorization signal is entered into the data input apparatus. The authorization signal is transmitted from the data input apparatus to the authorization computer. The validity of the authorization signal is verified in the authorization computer. A connection is established between the data input apparatus and a receiver unit upon verification of the validity of the authorization signal.

The authorization signal can be transmitted from the data input apparatus to the authorization computer along the first transmission path.

Acceptance of the authorization signal during verification of the validity of the authorization signal by the authorizing computer can be limited to a predefined number of times, to a predefined user time,

depending on a predetined number of data files being transmitted, or depending on a predefined size value of data files being transmitted.

A password can be employed for allowing accessing a member selected from the group consisting of the data input apparatus, the monitor, and the receiver unit.

The data transmitted from the data input apparatus to the receiver unit and vice versa or to the authorization computer and vice versa can be encoded.

An apparatus for authorizing access to a communication line includes a data input apparatus. An authorization computer is connected through a first transmission path to the data input apparatus. A monitor is connected to the authorization computer and disposed such that upon reading of an authorization signal on a monitor by a user, the user can enter the authorization signal into the data input apparatus. A receiver unit is connectable to the data input apparatus through a line switchable by the authorization computer between a connected state and a disconnected state.

The monitor can be a member selected from the group consisting of a pager, a handy, an email address, a net address, a telefax machine, a language output apparatus, an audio reproduction unit, a radio receiver, and a telephone.

The monitor can be a radio receiver incorporated into the data input apparatus. The radio receiver can furnish the authorization signal on a display monitor of the data input apparatus.

The radio receiver can include a user identification element furnished by a member selected from the group consisting of a magnetic card reader, a chip card reader, a graphic device for finger-print identification, and a graphic device for picture

identification.

A first encoding module can be present in the authorization computer. A second encoding module can be present in the monitor. The encoding provided by the first encoding module matches the encoding of the second encoding module.

The receiver unit can furnish a door-locking mechanism.

The authorization computer and the receiver unit can be integrated into a single apparatus. Furthermore, the data input apparatus, the authorization computer, and the receiver unit can be integrated into one single apparatus.

Wireless telecommunication apparatuses, such as for example Handys (Handie-Talkie is a tradename of the Motorola Communications Division) or pagers, are frequently furnished with the possibility to receive short alphanumeric communications, for example of the Short Message Service known in Germany as SMS-DIENST, and to display these communications on their display screen. A paging system is a communications system for summoning individuals such as doctors and nurses or for making public announcements. The present invention employs this possibility to receive short alphanumeric communications in order to transmit a transaction authorization number or a comparable password.

In accordance with the first aspect of the present invention. the user transmits his or her identification, such as user identification, password, or the like, and/or an identification characterization of the data input apparatus together with a request for generating a transaction authorization number TAN, or a comparable password, to a computer through a data input apparatus. The computer furnishes the authorization process and is therefore called in the following by the abbreviation

authorizing computer. An alphanumeric or only numeric transaction authorization number TAN, or a comparable password, is calculated or read from a data file based on a random number generator in this authorization computer. This transaction authorization number TAN, or a similar password, is transmitted to a receiver by the authorizing computer through another transmission path disposed parallel to the existing connection with the data-input apparatus. This receiver can be for example:

a) a wireless receiver with a display or a monitor such as for example a handy, a pager (for example a city-call receiver),

b) a specially constructed receiver card within the data input apparatus, which is accessed wirelessly or through a fixed wiring;

c) a mailbox;

d) a telefax apparatus; or

e) a language output apparatus such as a fixed installed audio speaker or a telephone for the language transmission.

The authorization computer includes a memory storage and has available the required telephone numbers, wireless call numbers, or fax numbers, email addresses or network addresses. The data reterring to this are usually stored in the authorization computer. However, it is possible that the authorization computer in turn shares and/or retrieves these data from a data source, which data source is resident on another computer. In addition, the authorization computer can also access this other computer on its own by using the method according to the present invention.

The authorized user can enter the thus transmitted transaction authorization number or the comparable password manually into his/her data input apparatus and send the transaction authorization number TAN again to

the authorization computer. An automatic transmission of the transaction authorization number TAN or of the comparable password occurs according to the present invention in case of an automatic procedure. The authorization computer checks and verifies now the congruence and agreement between all valid transaction authorization numbers TANs or comparable passwords previously given out by the authorizing computer, and the authorization computer allows a release of the data flow between the data input apparatus and a receiver unit after this checking of the authorization.

The transaction authorization number or the comparable password can be a transaction authorization number for one single use. However, other limitations such as the user time and/or the number or the size of the data files to be transmitted relating are also conceivable for use in determining the validity of the transaction authorization number or of the comparable password.

Now, data can be transmitted from the data input apparatua to the receiver unit and vice versa, for example by full duplex, after a connection authorized in the above described manner has been established.

It is clear that these data can also be encrypted or encoded first and then transmitted for obtaining additional security.

Both the data input apparatus, as well as the authorization computer and the receiver unit can be furnished as standard personal computers. The present invention operates independent from the platform employed, i.e. independent of the type of processor, of the operating system and/or of the control electronics, for example of the receiver unit, and/or of the input/output units, for example of the data input apparatus and of the receiver unit.

The security of this system is based on the fact that a data transmission from the data input apparatus to the receiver unit has to be released and turned on by the authorization computer only in case of an authorization of the apparatus. This is accomplished by the employment of separate transmission paths between the data input apparatus and the authorization computer on the one hand, and between the authorization computer and the transaction-authorization-number transmission on the other hand. The present invention is insofar distinguished from call-back systems, where only one checking occurs between the data input apparatus and the authorization computer.

The method according to a first aspect of the present invention allows to provide a number of different levels of security.

A wireless receiver, for example in the form of a plug-in card, is incorporated as a receiver in the data input apparatus, representing the lowest security level such that a data transmission is possible to the receiver unit only with this concrete apparatus. In order to increase this security, it can be provided that this wireless receiver can only be operated with a user identification element, for example a magnetic card or a chip card. The user identification element can also operate with graphical methods, such as testing, verification and/or identification of a fingerprint or of a picture identification of the user.

The further security level provides that the authorization computer transmits the transaction authorization number or the comparable password to a pager or a comparable apparatus. In this case, an authorization is furnished only when the data input apparatus and the pager are accessed by the same person. Only then is it possible that the transaction authorization number or a

comparable password, displayed on the pager, are entered into the data input apparatus and are transmitted from there again to the authorization computer.

Data transmitted to a pager can however be branched off and be listened to. A further security step can be obtained in the manner that matching encoding or encryption modules are employed in the authorization computer and in the pager.

Another receiver apparatus can be furnished instead of the pager or the handy. This can for example be a mailbox, a telefax, a language output apparatus, a sound-receiver printed circuit board or an audio-response unit. Fixedly installed audio speakers or the transmission of the audio or voicemail to a defined telephone connection are possible to serve as an audio output unit and audio-response unit. An audio output of the transaction authorization number or of the comparable password is performed with the language output apparatus or audio-response unit.

The transmission to such receiver apparatuses can also be encoded and/or encrypted.

Further encoding mechanisms can be dispensed with if one employs a handy, in particular a GSM handy, instead of a pager based on the encoding of the respective transmission technique. In this case, the display of the transaction authorization number or of the comparable password is performed on the display of the handy.

A further step of security can be accomplished by establishing a connection between the data input apparatus and the authorization computer only when a corresponding password is transmitted through the data input apparatus. This password can be valid according to the present invention for a time, which is substantially longer than the transfer authorization number TAN.

A further step of security can be achieved by, requiring also a password already for the use of the data

input apparatus.

It is apparent that a combination of the precedingly recited step of security is possible.

In accordance with a second aspect of the present invention there is provided an apparatus for authorizing access to a communication line comprising a data input apparatus, an authorization computer connected through a first transmission path to the data input apparatus, a monitor connected to the authorization computer and disposed such that upon reading of an authorization signal on a monitor by a user, the user can enter the authorization signal into the data input apparatus; a receiver unit connectable to the data input apparatus through a line switchable by the authorization computer between the connected state and a disconnected state.

The present invention can be universally employed in the region of data transmission systems. This holds for example also for the Internet and intranets, local area networks LAN, wide area networks WAN, etc.

The system in question can also be employed outside of the classic electronic data processing, for example in connection with physical access controls. For this purpose, the user enters for example his or her personal password on a keyboard, representing a data input apparatus, and located next to a door. The authorization computer checks and verifies this password, possibly also in connection with the access permission to the concrete space at the concrete time. If the respective password is still valid, then the authorization computer provides the transaction authorization number or the comparable password to a handy or to an apparatus conceived for the special door closing system and functionally comparable with the pager. In the following, this transaction authorization number or the comparable password is

entered manually by the user to a keyboard disposed in proximity of the door and is further transmitted automatically to the authorization computer. After a successful verification, a signal is provided by the authorization computer for a release of the door-locking mechanism. The release can be limited in time, if desired. The receiver unit can in this case be of the most simple nature relative to its technological construction, since the receiver unit only has to process the signal for the release of the door-locking mechanism in such a way that the respective electro-mechanical system releases the door for opening.

Thus, it is possible to construct a system where different persons have different authorizations for accessing different rooms.

The concrete fields of application comprise, for example:

computer centers
airports
ministries, government offices
customs
border transition points
security regions
banks
police and military applications
shielded storage, vaults, bank vaults
garages
parking houses
automobiles

The complete system receives its security from the combination of several different base principles and factors:

(1) "what you have" (the GSM chip card riot to be duplicated), i.e. a physically unique structure which

cannot be transferred without loss.

(2) "what you know" (the PIN of the GSM chip card as well as the own user names in the data input apparatus and/or the authentication server), i.e. know-how which cannot be transferred without intent or by mistake.

(3) DES-encoding and cryptographic authentication in the GSM net itselfi whereby resistance against listening attacks and manipulating attacks is obtained.

The combination of at least three events, which events by themselves are already very improbable, is necessary for a compromising of the system;

a) physical loss of the handy chip card, of the pager, or a foreign access to the mailbox, to the telefax, to the language output apparatus, or to the audio-delivery unit,

b) giving out of the PIN number of the receiver (for example of the chip card or of the handy) and

c) knowledge of the transmitted transaction authorization number or of the comparable password.

An inadvertent coincidence of these factors is nearly excludable, since also in this case the successful attack on the system presupposes the intimate knowledge of the access procedure and of the user identification ID, which is usually not present in case of an attack. In addition, the user has the possibility to block immediately or to have blocked immediately his or her user identification ID at the authentication server upon a loss of his or her chip card.

A further advantage of the support of the GSM can be that the user is reachable all the time during the authorization process, i.e. the user can be directly called by the system administrator in case of access problems or doubts in regard to the identity of the user.

This solution is associated with the advantage that

the solution is very secure, low cost, and realizable with widely available and secure, conventional hardware.

A further solution according to the present invention comprises that the authorization computer and the receiver unit are present as a single apparatus.

The present invention may be more fully understood from the description of preferred embodiments given below with reference to the accompanying drawings, by way of example only.

Brief Description of the Drawings

In the accompanying drawing, in which are shown several of the various possible embodiments of the present invention:

Fig. 1 is a view of a schematic diagram showing an operational system employing authorization in data transmission.

Description of Invention and Preferred Embodiment

The user sends according to a first step his or her qualifying identification through a data input apparatus 1, together with a request for generating or for selecting a transaction authorization number TAN or a comparable password from a data file, to an authorization computer 2. The authorization computer 2 generates the transaction authorization number TAN or the comparable password or selects the transaction authorization number TAN or the comparable password from a data file according to a second step. The authorization computer 2 sends the transaction authorization number TAN or the comparable password through a different transmission path as compared to the transmission path of the first step to a receiver 3 according to a third step. The user takes this transaction authorization number TAN or the comparable password from the receiver 3 and enters the transaction authorization

number TAN or the comparable password into the data input apparatus 1 according to a fourth step. This transaction authorization number TAN or the comparable password is transmitted again to the authorization computer 2 according to a fifth step. The authorization computer 2 verifies the validity of the transaction authorization number TAN or of the comparable password according to a sixth step, in order to establish a connection between the data input apparatus 1 and a receiver unit 4 according to a seventh step.

The transaction authorization number TAN or the comparable password can be a one-time usable transaction authorization number TAN or a one time usable password. The validity of the transaction authorization number TAN or of the comparable password can be limited to a predefined user time. The validity of the transaction authorization number TAN or of the comparable password can be dependent on a predefined number of the transmitted data files or on a predefined size value of the transmitted data files.

Access to the data input apparatus 1 and/or to the receiver 3 and/or the receiver unit 4 can be protected by a password. The data transmitted from the data input apparatus 1 to the receiver unit 4 or vice versa can be encoded and the data transmitted from the data input apparatus 1 to the authorization computer 2 or vice versa are encoded.

The apparatus for the authorization of data transmission systems includes a data input apparatus 1 serving for entering a qualifying identification of a user into the data input apparatus 1 and for transmitting the qualifying identification and a request for an authorization signal from the data input apparatus 1 to the authorization computer 2 along a first transmission path. The authorization computer 2

serves for establishing the authorization signal in the authorization computer 2, and for sending the authorization signal from the authorization computer 2 to a monitor 3 along a second transmission path different as compared to the first transmission path. The monitor 3 serves for reading the authorization signal at the monitor 3 by the user. The data input apparatus 1 further serves for entering the authorization signal into the data input apparatus 1 by the user and for transmitting the authorization signal from the data input apparatus 1 to the authorization computer 2. The authorization computer 2 further serves for verifying the validity of the authorization signal in the authorization computer 2 and for establishing a connection between the data input apparatus 1 and the receiver unit 3 upon veriticatIon of the validity of the authorization signal.

The receiver 3 can be a pager 31 or a handy 32. The receiver 3 can also be an email address or a net address, a telefax machine 33, or a language output apparatus or an audio reproduction unit. The language output apparatus or the audio reproduction unit can be a loud and audio speaker 34 or a telephone 35.

The receiver 3 can be a radio receiver incorporated into the data input apparatus 1. The radio receiver can furnish the transaction authorization number TAN or the comparable password on the display or monitor of the data input apparatus 1. The radio receiver can include a user identification element.

The user identification element can be a magnetic card or a chip card. The user identification element can operate with graphic devices for verifying a finger print or for a picture identification of the user.

Matching encoding modules can be present in the authorization computer 2 and in the receiver 3.

The receiver element 4 can be a door-locking mechanism.

The authorization computer 2 and the receiver unit 4 can be integrated into a s]Lngle apparatus. The data input apparatus, the authorization computer 2, and the receiver unit 4 can be integrated into one single apparatus.

An authorized user actuates a data input apparatus 1. The authorized user enters and sends 101 a request tor generating or for selecting and returning a transaction authorization number TAN or a comparable password to an authorization computer 2 along a transmission path 102 from the data input apparatus 1 to the authorization computer 2. The authorization computer 2 generates a transaction signal such as the transaction authorization number TAN or a comparable password. The authorization computer 2 can derive the authorization signal from a random number generator 5 or from a data file contained in the authorization computer 2. The authorization computer 2 knows the telephone number or the data address, for example the email address or net address of the receiver 3 of the user of the data input apparatus 1. The authorization computer 2 sends this transaction authorization number TAN or a comparable password to a monitor representing the receiver 3 along a transmission path 103 from the authorization computer 2 to the monitor or receiver 3. The receiver 3 can be a pager 31 or a handy 32. The receiver 3 however can also be provided as the email address of a mailbox 37 and displayed on a monitor 36, a telefax apparatus 33, or a language output apparatus or audioreproduction unit. The audio-reproduction unit can be a fixedly installed audio speaker 34 or a telephone 35. The language output apparatus can be a computer 38 reconstituting language into sound or text

files.

The monitor can be a radio receiver incorporated into the data input apparatus, wherein the radio receiver furnishes the authorization signal on a display monitor of the data input apparatus. The radio receiver can include a user identification element furnished by an access card such as a magnetic card or a chip card.

The user reads this transaction authorization number or a comparable password from the receiver 3 or hears the transaction authorization number TAN from the language or audio output and enters 104 it manually into the data input apparatus 1. The data input apparatus 1 now transmits the transaction authorization number TAN or the comparable password to the authorization computer 2 along a transmission path 105 from the data input apparatus 1 to the authorization computer 2. The authorization computer 2 verifies if this transaction authorization number TAN or the comparable password are still valid. For this purpose, the authorization computer can be programmed such that the validity of the transaction authorization number or of the comparable password is limited in time between its emission to the receiver 3 and its transmission through the data input apparatus 1. The time period limitation can for example amount to two minutes. If the transaction authorization number TAN or the comparable password are valid, then the authorization computer 2 furnishes a connection 107, 108 from the data input apparatus 1 to the receiver unit 4. Now the user is able to transmit and/or to receive data from the data input apparatus 1 to the receiver unit 4 for the time period this connection 107, 108 is maintained.

It is apparent that these data can be encrypted and encoded for additional security.

It is further conceivable that not only the transaction authorization number TAN or the comparable password have a time limitation with respect to their validity, but that also the time duration of the maintaining of the connection 107, 108 between the data input apparatus 1 and the receiver apparatus 4 is limited in time. Thereby, it can be avoided that a "standing" line is furnished between the data input apparatus 1 and the receiver unit 4, which gain could represent a hole in the security system.

The authorization computer 2 and the receiver uni-t 4 can be furnished by a single computer. In this case, a first access is performed to a data processing program, which performs the authorization process, including generation and transmission of the transaction authorization number TAN, in the manner precedingly described. The data transmission is then performed as a second step.

The data input apparatus 1, the authorization computer 2 and the receiver unit 4 can even be a single computer. in this case, a first access is performed to a data processing program, which performs the authorization process, including generation and transmission of the transaction authorization number TAN, to the receiver in the way described above. The user obtains full access to or access limited to specific regions of the computer only after authorization.

It will be understood that each of the elements described above, or two or more together, may also find a useful application in other types of authorization processes differing from the types described above.

While the invention has been illustrated and described as embodied in the context of a method for the authorization in data transmission systems, it is

not intended to be limited to the details shown, since various modifications and structural changes may be made without departing in any way from the spirit of the present invention.

Without further analysis, the foregoing will so fully reveal the gist of the present invention that others can, by applying current knowledge, readily adapt it for various applications without omitting features that, from the standpoint of prior art, fairly constitute essential characteristics of the generic or specific aspects of this invention.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A method for the authorization of data transmission systems comprising

entering a qualifying identification of a user into a data input apparatus;

transmitting the qualifying identification and a request for an authorization signal from the data input apparatus to an authorization computer along a first transmission path;

establishing the authorization signal in the authorization computer;

sending the authorization signal from the authorization computer to a monitor along a second transmission path different as compared to the first transmission path;

reading the authorization signal at the monitor by the user;

entering the authorization signal into the data input apparatus;

transmitting the authorization signal from the data input apparatus to the authorization computer. verifying the validity of the authorization signal in the authorization computer;

establishing a connection between the data input apparatus and a receiver unit upon verification of the validity of the authorization signal.

2. The method according to claim 1 wherein the authorization signal is transmitted from the data input apparatus to the authorization computer along the first transmission path.

3. The method according to claim 1 or 2; further comprising limiting acceptance of the authorization signal during verification of the validity of the authorization signal by the authorizing computer to a predefined number of times.

4. The method according to any one of the preceding claims, further comprising limiting acceptance of the authorization signal during verification of the validity of the authorization signal by the authorizing computer to a predefined user time.

5. The method according to any one of the preceding claims, further comprising limiting acceptance of the authorization signal during verification of the validity of the authorization signal by the authorizing computer depending on a predefined number of data files being transmitted.

6. The method according to any one of the preceding claims, further comprising limiting acceptance of the authorization signal during verification of the validity of the authorization signal by the authorizing computer depending on a predefined size value of data files being transmitted.

7. The method according to any one of the preceding claims further comprising employing a password for allowing accessing a member selected from the group consisting of the data input apparatus, the monitor, and the receiver unit.

8. The method according to any one of the preceding claims, further comprising encoding the data transmitted from the data input apparatus to the receiver unit and vice versa.

9. The method according to any one of the preceding claims, further comprising encoding the data transmitted from the data input apparatus to the authorization computer and vice versa.

10. A method for the authorization of data transmission systems employing a transaction authorization number (TAN) or a comparable password,
wherein a user sends according to a first step his or her qualifying identification through a data input apparatus,

together with a request for generating or for selecting a transaction authorization number TAN or a comparable password from a data file, to an authorization computer, wherein the authorization computer generates the transaction authorization number TAN or the comparable password or selects the transaction authorization number TAN or the comparable password from a data file according to a second step, wherein the authorization computer sends the transaction authorization number TAN or the comparable password through a different transmission path as compared to the transmission path of the first step to a receiver according to a third step, wherein the user takes this transaction authorization number TAN or the comparable password from the receiver and enters the transaction authorization number TAN or the comparable password into the data input apparatus according to a fourth step, wherein thistransaction authorization number TAN or the comparable password is transmitted again to the authorization computer according to a fifth step, wherein the authorization computer verifies the validity of the transaction authorization number TAN or of the comparable password according to a sixth step, in order to establish a connection between the data input apparatus and a receiver unit according to a seventh step.

11. The method according to claim 10, wherein the transaction authorization number TAN or the comparable password is a one-time usable transaction authorization number TAN or a one time usable password; wherein the validity of the transaction authorization number TAN or of the comparable password is limited to a predefined user time; wherein the validity of the transaction authorization number TAN or of the comparable password is dependent on a predefined number of the transmitted data files; wherein the validity of the transaction authorization number TAN or of the comparable password is dependent on a predefined

size value of the transmitted data files.

12. The method according to claim 10, wherein access to the data input apparatus and/or to the receiver and/or the receiver unit is protected by a password; wherein the data transmitted from the data input apparatus to the receiver unit or vice versa are encoded; wherein the data transmitted from the data input apparatus to the authorization computer or vice versa are encoded.

13. An apparatus for authorizing access to a communication line comprising a data input apparatus; an authorization computer connected through a first transmission path to the data input apparatus; a monitor connected to the authorization computer and disposed such that upon reading of an authorization signal on a monitor by a user, the user can enter the authorization signal into the data input apparatus; a receiver unit connectable to the data input apparatus through a line switchable by the authorization computer between a connected state and a disconnected state.

14. The apparatus according to claim 13, wherein the monitor is a member selected from the group consisting of a pager, a handy, an email address, a net address, a telefax machine, a language output apparatus, an audio reproduction unit, a radio receiver, and a telephone.

15. The apparatus according to claim 13 or 14, wherein the monitor is a radio receiver incorporated into the data input apparatus, wherein the radio receiver furnishes the authorization signal on a display monitor of the data input apparatus.

16. The apparatus according to any one of claims 13-15 wherein the radio receiver includes a user identification element furnished by a member selected from the group consisting of a magnetic card reader, a chip card reader, a graphic device for finger-print identification, and a graphic device for picture identification.

17. The apparatus according to any one of claims 13-16 comprising a first encoding module present in the authorization computer; a second encoding module present in the monitor, wherein an encoding provided by the first encoding module matches an encoding of the second encoding module.

18. The apparatus according to any one of claims 13-17, wherein the receiver unit furnishes a door-locking mechanism.

19. The apparatus according to any one of claims 13-18, wherein the authorization computer and the receiver unit are integrated into a single apparatus.

20. The apparatus according to any one of claims 13-19, wherein the data input apparatus, the authorization computer, and the receiver unit are integrated into one single apparatus.

21. The apparatus according to any one of claims 13-20, wherein the data input apparatus serves for entering a qualifying identification of a user into the data input apparatus and for transmitting the qualifying identification and a request for an authorization signal from the data input apparatus to the authorization computer along a first transmission path; wherein the authorization computer serves for establishing the authorization signal in the authorization computer, and for sending the authorization signal from the authorization computer to a monitor along a second transmission path different as compared to the first transmission path; wherein the monitor serves for reading the authorization signal at the monitor by the user; wherein the data input apparatus further serves for entering the authorization signal into the data input apparatus by the user and for transmitting the authorization signal from the data input apparatus to the authorization computer; wherein the authorization computer further serves for verifying the validity of the

authorization signal in the authorization computer and for establishing a connection between the data input apparatus and the receiver unit upon verification of the validity of the authorization signal.

22. A method for authorization of data transmission systems substantially as herein described with reference to the accompanying drawing.

23. An apparatus for authorizing access to a communication line substantially as herein described with reference to the accompanying drawing.

Dated this 22nd day of April 1998

KIM SCHMITZ

By his Patent Attorney

GRIFFITH HACK

ABSTRACT OF THE DISCLOSURE

The invention relates to a method and to a device for the authorization in data transmission systems employing a transaction authorization number (TAN) or a comparable password. According to a first step, the user sends a qualifying identification of the data input apparatus together with a request for the generation or for the selection of a transaction authorization number TAN or of comparable password from a data file from the data input apparatus to an authorization computer. In a second step the authorization computer generates the transaction authorization number TAN or the comparable password or selects them form a data file. According to a third step, the authorization computer sends the transaction authorization number TAN or the comparable password over a second transmission path different from the first transmission path to a monitor, for example a handy or a pager. According to a fourth step, the user reads this transaction authorization number TAN or the comparable password from the receiver and enters the transaction authorization number TAN or the comparable password into the data input apparatus. According to a fifth step, this transaction authorization number TAN or the comparable password is transmitted to the authorization computer. According to a sixth step, the authorization computer verifies the validity of the transaction-authorization number TAN or of the comparable password in order to establish or switch free, according to a seventh step, a connection between the data input apparatus and the receiver unit.

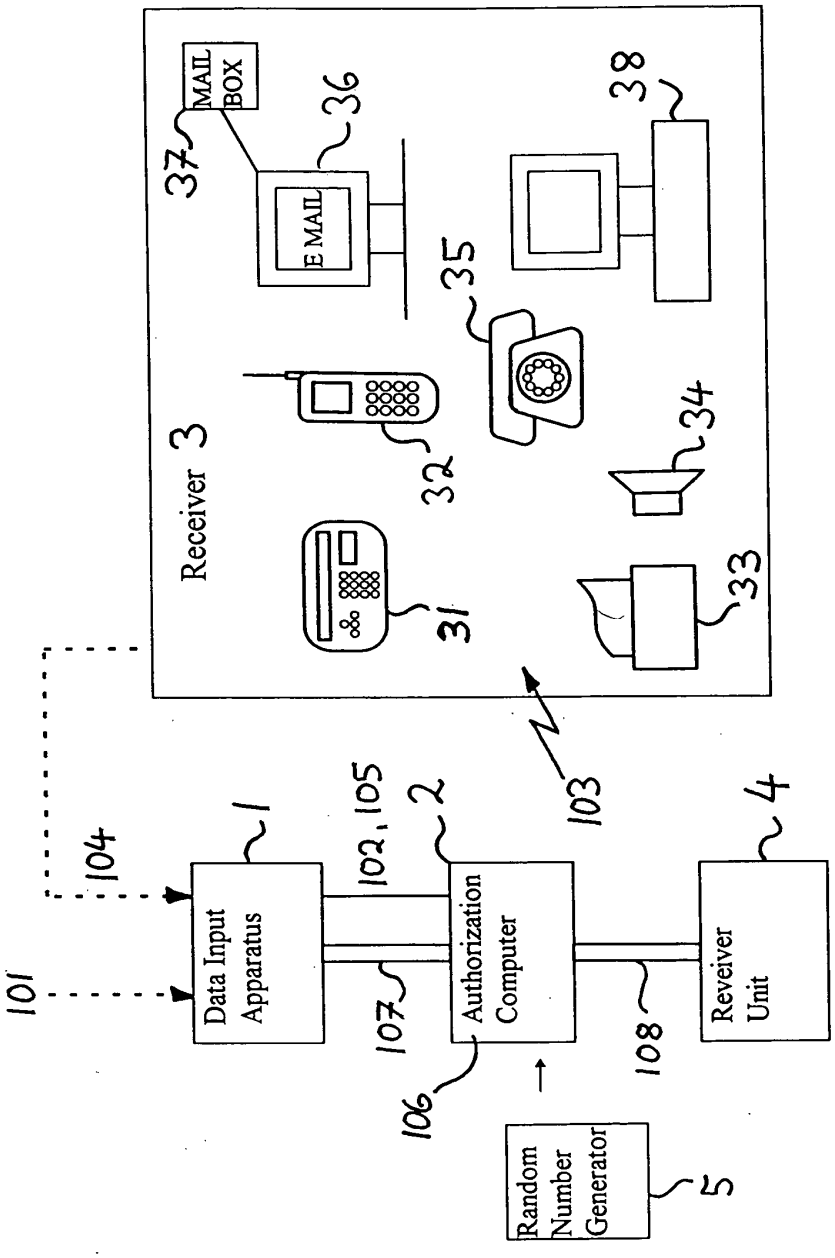

Receiver 3
MAIL BOX
37
E MAIL
36
38
35
34
32
31
33
103
104
101
1
Data Input Apparatus
102, 105
2
Authorization Computer
4
Reveiver Unit
107
108
106
Random Number Generator
5

Fig. 1

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 875 871 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
04.11.1998 Patentblatt 1998/45

(51) Int. Cl.[6]: **G07F 19/00**, G07F 7/10, G07C 9/00

(21) Anmeldenummer: **98100688.5**

(22) Anmeldetag: **16.01.1998**

(84) Benannte Vertragsstaaten:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **29.04.1997 DE 19718103**

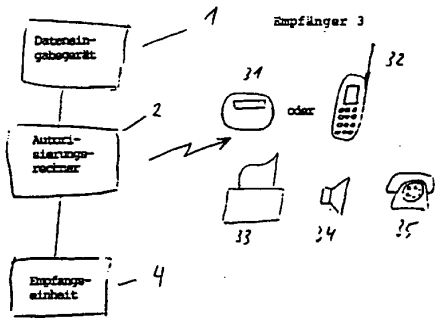
(71) Anmelder: **Schmitz, Kim**
80539 München (DE)

(72) Erfinder: **Schmitz, Kim**
80539 München (DE)

(74) Vertreter:
Freiherr von Gravenreuth, Günter, Dipl.-Ing. (FH)
Schwanthalerstrasse 3
80336 München (DE)

(54) Verfahren zur Autorisierung in Datenübertragungssystemen

(57) Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Autorisierung in Datenübertragungssystemen unter Verwendung einer Transaktionsnummer (TAN) oder eines vergleichbaren Paßworts, wobei der Benutzer in einem 1.Schritt über ein Dateneingabegerät seine Identifizierung und/oder eine Identifizierungs-Kennung des Dateneingabegeräts zusammen mit der Aufforderung zur Generierung oder zur Auswahl einer TAN oder ein vergleichbaren Paßwort aus einer Datei an einen Autorisierungsrechner sendet, in einem 2. Schritt der Autorisierungsrechner die TAN oder das vergleichbare Paßwort generiert oder aus einer Datei auswählt, in einem 3. Schritt der Autorisierungsrechner die TAN oder das vergleichbares Paßworts über einen anderen Übertragungsweg als in Schritt 1 an einen Empfänger (z. B. Handy oder Pager) sendet, in einem 4. Schritt der Benutzer diese TAN oder das vergleichbare Paßwort von dem Empfänger übernimmt und in das Dateneingabegerät eingibt, in einem 5. Schritt diese TAN oder das vergleichbare Paßwort wieder an den Autorisierungsrechner übermittelt wird, in einem 6. Schritt der Autorisierungsrechner die Gültigkeit der TAN oder des vergleichbaren Paßworts prüft, um dann in einem 7. Schritt einen Verbindungsaufbau zwischen dem Dateneingabegerät und einer Empfangseinheit herzustellen oder freizuschalten.



EP 0 875 871 A2

Printed by Xerox (UK) Business Services
2.16.3/3.4

Beschreibung

Die Erfindung betrifft ein Verfahren zur Autorisierung in Datenübertragungssystemen.

Es ist bekannt, daß beim Telebanking der Benutzer neben seinem permanenten Passwort (PIN) für jede einzelne Transaktion noch zusätzlich eine Transaktionsnummer (TAN) benötigt. Derartige TAN's werden in größeren Blöcken dem Benutzer mit der Post übermittelt. Es besteht daher das Risiko, daß Dritte von derartigen TAN's Kenntnis erlangen und in Verbindung mit dem Passwort einen Mißbrauch vornehmen können. Das Risiko wird dadurch erhöht, daß derartige TAN's faktisch eine zeitlich unbegrenzte Gültigkeit besitzen.

Bekannt sind ferner Call-Back-Systeme, bei denen das angerufene System sich durch einen Rückruf bei einer im Regelfall gespeicherten Nummer vergewissert, daß das anrufende System autorisiert ist und nicht ein fremdes System sich für ein berechtigtes System ausgibt. Der Nachteil der Call-Back-Systeme besteht darin, daß ein unbefugter Benutzer, welcher sich aus einer beliebigen Quelle einen funktionalen Zugang zu dem berechtigten anrufenden System verschafft hat, unter dieser rechtswidrig erlangten Berechtigung problemlos arbeiten kann, da das Call-Back-System nur überprüft, ob es von einem grundsätzlich berechtigten System aus angerufen wurde.

Der Erfindung liegt die Aufgabe zugrunde ein Verfahren zur Autorisierung in der Datenübertragung zu schaffen, in dem die Sicherheit erhöht wird. Dieses Verfahren wird erfindungsgemäß durch den kennzeichnenden Teil des Anspruchs 1) gelöst.

Drahtlose Telekommunikationsgeräte wie beispielsweise Handys oder Pager besitzen oft die Möglichkeit, kurze (alpha-)numerische Nachrichten (z. B. der Short Message Service = SMS-Dienst) zu empfangen und auf ihrem Display anzuzeigen. Die vorliegende Erfindung nutzt diese Möglichkeit, um eine TAN oder ein vergleichbares Paßwort zu übermitteln.

Nach der vorliegenden Erfindung übermittelt der Benutzer über ein Dateneingabegerät seine Identifizierung (User-ID, Paßwort o. ä.) und/oder eine Identifizierungs-Kennung des Dateneingabegeräts zusammen mit einer Aufforderung zur Generierung einer TAN (oder eines vergleichbaren Paßworts) an einen Rechner, welcher den Autorisierungsvorgang übernimmt und nachfolgend kurz Autorisierungsrechner genannt wird. In diesem Autorisierungsrechner wird durch einen Zufallsgenerator eine alphanumerische oder nur numerische TAN (oder eine vergleichbares Paßwort) errechnet oder einer Datei entnommen. Dann wird von dem Autorisierungsrechner parallel zur bestehenden Verbindung mit dem Dateneingabegerät, über einen anderen Übertragungsweg diese TAN (oder ein vergleichbares Paßwort) an einen Empfänger übermittelt. Dieser Empfänger kann beispielsweise

a) ein Funkempfänger mit einem Display oder Monitor wie z. B. ein Handy, ein Pager (z. B. einen Cityruf-Empfänger),

b) eine speziell gestaltete Empfangskarte innerhalb des Dateneingabegerätes, welche über Funk oder eine feste Verdrahtung angesprochen wird,

c) eine Mailbox,

d) ein Telefax- oder

d) ein Sprachausgabegerät wie ein fest instalierter Lautsprecher oder ein (Sprach-)Telefon

sein. Hierzu verfügt der Autorisierungsrechner über die erforderliche(n) Telefon-, Funkruf- oder Faxnummern, E-Mail- oder Netzadresse(n). Die diesbezüglichen Daten sind üblicherweise im Autorisierungsrechner gespeichert. Es ist jedoch möglich, daß der Autorisierungsrechner seinerseits sich diese Daten aus einer Datenbank holt, welche sich auf einem anderen Rechner befindet. Insoweit kann auch der Autorisierungsrechner unter Verwendung des erfindungsgemäßem Verfahrens von sich aus einen Zugriff auf diesen anderen Rechner tätigen.

Der berechtigte Benutzer kann die ihm so übermittelte TAN (oder das vergleichbare Paßwort) manuell in sein Dateneingabegerät eingeben und wieder an den Autorisierungsrechner versenden. Bei automatisierten Verfahren erfolgt erfindungsgemäß eine automatische Übertragung der TAN (oder des vergleichbare Paßworts). Der Autorisierungsrechner überprüft nunmehr die Übereinstimmung zwischen allen (von ihm vergebenen) gültigen TAN's (oder vergleichbaren Paßwörtern) und ermöglicht nach dieser Autorisierungsprüfung eine Freigabe des Datenflusses zwischen dem Dateneingabegerät und einer Empfangseinheit.

Bei der TAN (oder dem vergleichbaren Paßwort) kann es sich um eine nur einmal verwendbare TAN handeln. Es sind jedoch auch andere Begrenzungen wie die Benutzerzeit und/oder die Zahl oder Größe der übertragenen Dateien für die Gültigkeit der TAN (oder des vergleichbaren Paßworts) denkbar.

Nach dem in vorgenannter Weise autorisierten Verbindungsaufbau können nunmehr Daten von dem Dateneingabegerät an die Empfangseinheit (oder umgekehrt; Volldublex) übermittelt werden.

Es liegt auf der Hand, daß zur zusätzlichen Sicherheit diese Daten auch verschlüsselt werden können.

Sowohl das Dateneingabegerät, als auch der Autorisierungsrechner und die Empfangseinheit können normale (Personal-)Computer sein. Die Erfindung arbeitet plattformunabhängig, d. h. sie ist unabhängig von Prozessortypen, Betriebssystemen und/oder Steuerelektroniken (z. B. der Empfangseinheit) und/oder Input/Output-Einheiten (z. B. des Dateneingabegeräts und der Empfangseinheit).

Die Sicherheit dieses Systems liegt darin, daß nur bei einer Autorisierung der Geräte eine Datenübertragung von dem Dateneingabegerät an die Empfangseinheit durch den Autorisierungsrechner freigeschaltet wird. Dies wird durch den Einsatz getrennter Übertra-

gungswege zwischen dem Dateingabegerät und dem Autorisierungsrechner einseits und dem Autorisierungsrechner und der TAN-Übertragung andererseits, erreicht. Insoweit unterscheidet sich die Erfindung von Call-Back-Systemen bei denen nur eine Überprüfung zwischen dem Dateneingabegerät und dem Autorisierungsrechner erfolgt.

Das erfindungsgemäße Verfahren ermöglicht verschiedenste Sicherheitsstufen.

Auf dem niedrigsten erfindungsgemäßen Sicherheitsniveau wird in dem Dateneingabegerät als Empfänger ein Funkempfänger beispielsweise in Form einer Steckkarte eingebaut, so daß nur mit diesem konkreten Gerät eine Datenübertragung an die Empfangseinheit möglich ist. Zur Erhöhung dieser Sicherheit kann vorgesehen werden, daß dieser Funkempfänger nur mit einem Benutzer-Identifizierungelement, beispielsweise einer Magnet- oder Chipkarte betrieben werden kann. Das Benutzer-Identifizierungelement kann auch mit grafischen Methoden wie Überprüfung eines Fingerabdruckes oder Bildidentifizierung des Benutzers arbeiten.

Die weitere erfindungsgemäße Sicherheitsstufe besteht darin, daß der Autorisierungsrechner die TAN (oder das vergleichbare Paßwort) an einen Pager oder ein vergleichbares Gerät übermittelt. In diesem Fall erfolgt eine Autorisierung nur dann, wenn das Dateneingabegerät und der Pager im Zugriff derselben Person sind. Nur dann ist es möglich, daß die auf dem Display des Pagers angezeigte TAN (oder ein vergleichbares Paßwort) in das Dateneingabegerät eingegeben und von dort wieder an den Autorisierungsrechner übermittelt wird.

Auf einen Pager übermittelte Daten können bekannterweise jedoch abgehört werden. Eine weitere erfindungsgemäße Sicherheitsstufe kann in der Weise erzielt werden, daß im Autorisierungsrechner und im Pager übereinstimmende Verschlüsselungs-Module im Einsatz sind.

Anstelle des Pagers oder Handys kann auch in erfindungsgemäßer Weise ein anderes Empfangsgerät vorgesehen sein. Dies kann eine Mailbox, ein Telefax oder ein Sprachausgabegerät sein. Als Sprachausgabegerät sind erfindungsgemäß fest installierte Lautsprecher oder die Übertragung der Sprache auf einen definierten Telefonanschluß möglich. Bei den Sprachausgabengeräten erfolgt eine sprachliche Ausgabe der TAN (oder des vergleichbaren Paßworts).

Es liegt auf der Hand, daß auch die Übertragung auf derartige Empfangsgeräte verschlüsselt werden kann.

Wenn anstelle eines Pagers ein Handy, insbesondere ein GSM-Handy, im Einsatz ist, dann kann man infolge der Verschlüsselung der diesbezüglichen Übertragungstechnik erfindungsgemäß auf weitere Verschlüsselungsmechanismen verzichten. In diesem Fall erfolgt die Anzeige der TAN (oder des vergleichbaren Paßworts) auf dem Display des Handys.

Eine weitere erfindungsgemäße Sicherheitsstufe kann dadurch erreicht werden, daß zwischen dem Dateneingabegerät und dem Autorisierungsrechner eine Verbindung nur dann aufgebaut wird, wenn über das Dateneingabegerät ein entsprechendes Passwort übermittelt wird. Dieses Passwort kann erfindungsgemäß eine wesentlich längere zeitliche Gültigkeit besitzen als die TAN.

Eine weitere erfindungsgemäße Sicherheitsstufe kann dadurch erreicht werden, daß bereits zur Benutzung des Dateneingabegerätes ebenfalls ein Passwort erforderlich ist.

Es liegt auf der Hand, daß eine Kombination der vorgenannten Sicherheitsstufen möglich ist.

Die Erfindung ist universell im Bereich der Datenübertragungssysteme einsetzbar. Dies gilt beispielsweise auch für das Internet und Intra-Netze, Local-Area-Networks (LAN), Wide-Area-Networks (WAN) etc..

Das fragliche System ist auch außerhalb der klassischen EDV beispielsweise bei physischen Zugangskontrollen einsetzbar. Der Benutzer gibt hierzu beispielsweise auf einer in Türnähe angebrachten Tastatur (= Dateneingabegerät) sein persönliches Passwort ein. Der Autorisierungsrechner prüft dieses Passwort, ggfs. auch in Verbindung mit der Zugangsberechtigung zu dem konkreten - zur konkreten Zeit - Raum. Wenn das betreffende Passwort (noch) gültig ist, übermittelt der Autorisierungsrechner an ein Handy oder ein für das spezielle Türschließ-System konzepierte, funktional mit einem Pager vergleichbares Gerät, die TAN (oder das vergleichbare Paßwort). Anschließend wird diese TAN (oder das vergleichbare Paßwort) vom Benutzer manuell über die in Türnähe angebrachte Tastatur eingegeben und automatisch an den Autorisierungsrechner weitergeleitet. Nach erfolgreicher Überprüfung erfolgt vom Autorisierungsrechner ein Signal für die Freigabe des Türschließ-Mechanismus. Diese Freigabe kann ggfs. zeitlich begrenzt sein. Die Empfangseinheit kann in diesem Fall in technischer Hinsicht einfachster Natur sein, da sie nur das Signal für die Freigabe des Türschließ-Mechanismus so verarbeiten muß, daß die betreffende Elektro-Mechanik die Türe zum Öffnen freigibt.

So ist es möglich ein System aufzubauen, bei dem unterschiedliche Personen unterschiedliche Berechtigung zur Betretung verschiedener Räume haben.

Die konkreten Anwendungsfelder umfassen, z.B.:

- Rechenzentren
- Flughäfen
- Ministerien
- Zoll
- Grenzübergänge
- Sicherheitsbereiche
- Banken
- Tresore
- Garagen

- Parkhäuser
- Autos

Das gesamte System erhält seine Sicherheit aus der Kombination mehrerer unterschiedlicher Basisprinzipien und Faktoren:

(1) "what-you-have" (die nicht zu duplizierende (GSM-)Chipkarte), also ein physisches Unikat, das nicht verlustfrei weitergegeben werden kann.

(2) "what-you-know" (die PIN der GSM-Chipkarte sowie den eigenen Benutzernamen im Dateneingabegerät und/oder Authentifizierungsserver), also Know-How, das nicht unabsichtlich oder versehentlich weitergegeben werden kann

(3) DES-Verschlüsselung und kryptografische Authentifikation im GSM-Netz selbst, dadurch Resistenz gegen Abhör- und Manipulationsangriffe

Dadurch ist zur Kompromittierung des Systems die Kombination mindestens dreier - jeweils für sich schon sehr unwahrscheinlicher - Ereignisse von nöten:

a) physischer Verlust der (Handy-)Chipkarte, des Pagers oder ein fremder Zugriff auf die Mailbox, das Telefax-oder, Sprachausgabegerät,
b) Herausgabe der PIN des Empfängers (z. B. von der Chipkarte oder des Handy) und
c) Kenntnis der übermittelten TAN oder des vergleichbaren Paßwortes.

Ein versehentliches Zusammentreffen dieser Faktoren ist nahezu auszuschließen, zumal auch in diesem Fall der erfolgreiche Angriff auf das System die intime Kenntnis des Zugangsverfahrens und der Benutzer-ID voraussetzt, die bei einem Angriff im Normalfall nicht gegeben ist. Außerdem hat der Nutzer die Möglichkeit, seine Benutzer-ID bei Verlust seiner Chipkarte beim Authentifizierungsserver sofort zu sperren oder sperren zu lassen.

Ein weiterer Vorteil der Abstützung auf GSM besteht darin, daß der Benutzer während des Autorisierungsvorganges jederzeit erreichbar ist, also z.B. bei Zugangsproblemen oder Zweifeln an seiner Identität vom Systembetreuer direkt angerufen werden kann.

Diese Lösung hat den Vorteil, daß sie sehr sicher, kostengünstig und mit herkömmlicher, weit verbreiteter und sicherer Hardware realisierbar ist.

Eine weitere erfindungsgemäße Lösung besteht darin, daß Autorisierungsrechner und Empfangseinheit ein Gerät sind.

Weitere Vorteile und Anwendungsmöglichkeiten der Erfindung ergeben sich aus dem nachfolgend benannten Ausführungsbeispiel in Verbindung mit der Zeichnung.

Ein berechtigter Benutzer betätigt ein Dateneingabegerät 1). Hierüber sendet er die Aufforderung zur Generierung oder Auswahl und Rücksendung einer TAN (oder eines vergleichbaren Paßwortes) an einen Autorisierungsrechner 2). Der Autorisierungsrechner 2) generiert die TAN (oder ein vergleichbares Paßwort). Dem Autorisierungsrechner 2) ist die Rufnummer oder Datenadresse, z. B. die E-Mail- oder Netz-Adresse des Empfängers (3) des Benutzers des Dateneingabegerätes 1) bekannt. Er sendet an einen Empfänger 3) (nicht näher dargestellt) diese TAN (oder ein vergleichbares Paßwort). Der Empfänger 3) kann ein Pager 31) oder ein Handy 32) sein. Der Empfänger 3) kann jedoch auch die E-Mail-Adresse einer Mailbox (nicht dargestellt), ein Telefax-Gerät 33) oder ein Sprachausgabegerät sein. Das Sprachausgabegerät kann ein fest installierter Lautsprecher 34) oder ein Telefon 35) sein. Der Benutzer ließt diese TAN (oder ein vergleichbares Paßwort) vom Empfänger 3) ab oder hört sie von der Sprachausgabe und gibt sie manuell in das Dateneingabegerät 1) ein. Das Dateneingabegerät 1) übermittelt nunmehr die TAN (oder ein vergleichbares Paßwort) an den Autorisierungsrechner 2). Der Autorisierungsrechner 2) überprüft, ob diese TAN (oder das vergleichbare Paßwort) noch gültig ist. Zu diesem Zweck kann der Autorisierungsrechner so programmiert sein, daß die Gültigkeit der TAN (oder des vergleichbaren Paßworts) zwischen ihrer Versendung an den Empfänger 3) und ihre Übermittlung über das Dateneingabegerät 1) zeitlich begrenzt ist. Die zeitliche Begrenzung kann beispielsweise zwei Minuten betragen. Wenn die TAN (oder das vergleichbare Paßwort) gültig ist, dann stellt der Autorisierungsrechner 2) eine Verbindung zu einer Empfangseinheit 4) her. Nunmehr ist der Benutzer für die Dauer der Aufrechterhaltung dieser Verbindung in der Lage, Daten vom Dateneingabegerät 1) an die Empfangseinheit 4) zu übermitteln und/oder zu empfangen.

Es liegt auf der Hand, daß diese Daten zur weiteren Sicherung verschlüsselt werden können.

Denkbar ist ferner, daß nicht nur die TAN (oder das vergleichbare Paßwort) hinsichtlich ihrer Gültigkeit eine zeitliche Begrenzung hat, sondern daß auch die Dauer der Aufrechterhaltung der Verbindung zwischen dem Dateneingabegerät 1) und der Empfangseinheit 4) zeitlich begrenzt ist. Hierdurch kann vermieden werden, daß eine "Standleitung" zwischen dem Dateneingabegerät 1) und der Empfangseinheit 4) hergestellt wird, was wiederum eine Sicherheitslücke darstellen könnte.

Der Autorisierungsrechner 2) und die Empfangseinheit 4) können ein einziger Computer sein. In diesem Fall erfolgt ein erster Zugriff auf ein Datenverarbeitungsprogramm, welches den Autorisierungsvorgang (Generierung und Übermittlung der TAN) in vorgenannter Weise durchführt. In einem zweiten Schritt erfolgt dann die Datenübertragung.

Es können sogar das Dateneingabegerät (1), der Autorisierungsrechner 2) und die Empfangseinheit 4) ein einziger Computer sein. In diesem Fall erfolgt ein

erster Zugriff auf ein Datenverarbeitungsprogramm, welches den Autorisierungsvorgang (Generierung und Übermittlung der TAN an den Empfänger) in vorgenannter Weise durchführt. Erst nach der Autorisierung erhält der Benutzer einen vollen oder auf gewisse Bereiche beschränkten Rechnerzugang.

Bezugszeichenliste

Dateneingabegerät	1)
Autorisierungsrechner	2)
Empfänger	3)
Pager	31)
Handy	32)
Telefax-Gerät	33)
Lautsprecher	34)
Telefon	35)
Empfangseinheit	4)

Patentansprüche

1. Verfahren zur Autorisierung in Datenübertragungssystemen unter Verwendung einer Transaktionsnummer (TAN) oder eines vergleichbaren Paßworts, **dadurch** gekennzeichnet,

   - daß der Benutzer in einem 1.Schritt über ein Dateneingabegerät (1) seine Identifizierung und/oder eine Identifizierungs-Kennung des Dateneingäbegeräts (1) zusammen mit der Aufforderung zur Generierung oder zur Auswahl einer TAN oder eines vergleichbaren Paßworts aus einer Datei an einen Autorisierungsrechner (2) sendet,
   - daß in einem 2. Schritt der Autorisierungsrechner (2) die TAN oder das vergleichbare Paßwort generiert oder aus einer Datei auswählt,
   - daß in einem 3. Schritt der Autorisierungsrechner (3) die TAN oder das vergleichbare Paßwort über einen anderen Übertragungsweg als in Schritt 1 an einen Empfänger (3) sendet,
   - daß in einem 4. Schritt der Benutzer diese TAN oder das vergleichbare Paßwort von dem Empfänger (3) übernimmt und in das Dateneingabegerät (1) eingibt,
   - daß in einem 5. Schritt diese TAN oder das vergleichbare Paßwort wieder an den Autorisierungsrechner (2) übermittelt wird,
   - daß in einem 6. Schritt der Autorisierungsrechner (2) die Gültigkeit der TAN oder des vergleichbaren Paßworts prüft, um dann
   - in einem 7. Schritt einen Verbindungsaufbau zwischen dem Dateneingabegerät (1) und einer Empfangseinheit (4) herzustellen oder freizuschalten.

2. Verfahren nach Anspruch 1), dadurch gekennzeichnet, daß es sich um eine nur einmal verwendbare TAN oder eine vergleichbares Paßwort handelt.

3. Verfahren nach einem oder mehreren der Ansprüche 1) bis 2), dadurch gekennzeichnet, daß die Gültigkeit der TAN oder des vergleichbaren Paßworts eine vordefinierte Benutzerzeit ist.

4. Verfahren nach einem oder mehreren der Ansprüche 1) bis 3), dadurch gekennzeichnet, daß die Gültigkeit der TAN oder des vergleichbaren Paßworts von einer vordefinierten Anzahl der übertragenen Dateien abhängig ist.

5. Verfahren nach einem oder mehreren der Ansprüche 1) bis 4), dadurch gekennzeichnet, daß die Gültigkeit der TAN oder des vergleichbaren Paßworts von einer vordefinierten Größe der übertragenen Dateien abhängig ist.

6. Verfahren nach einem oder mehreren der Ansprüche 1) bis 5), dadurch gekennzeichnet, daß der Zugriff auf das Dateneingabegerät (1) und/oder der Empfänger (3) und/oder die Empfangseinheit (4) durch ein Passwort geschützt ist.

7. Verfahren nach einem oder mehreren der Ansprüche 1) bis 6), dadurch gekennzeichnet, daß die von dem Dateneingabegerät (1) an die Empfangseinheit(4) oder umgekehrt übermittelten Daten verschlüsselt sind.

8. Verfahren nach einem oder mehreren der Ansprüche 1) bis 7), dadurch gekennzeichnet, daß die von dem Dateneingabegerät (1) an den Autorisierungsrechner (2) oder umgekehrt übermittelten Daten verschlüsselt sind.

9. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 8), dadurch gekennzeichnet, daß der Empfänger 3) ein Pager (31) ist.

10. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 8), dadurch gekennzeichnet, daß der Empfänger 3) ein Handy (32) ist.

11. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 8), dadurch gekennzeichnet, daß der Empfänger 3) ein Telefax (33) ist.

12. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 8), dadurch gekennzeichnet, daß der Empfänger 3) eine E-Mail- oder Netzwerkadresse ist.

13. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 8), dadurch gekennzeichnet, daß der Empfänger 3) ein Sprachausgabegerät ist.

14. Vorrichtung nach Anspruch 11), dadurch gekennzeichnet, daß das Sprachausgabegerät ein Lautsprecher (34) ist.

15. Vorrichtung nach Anspruch 11), dadurch gekennzeichnet, daß das Sprachausgabegerät ein Telefon (35) ist.

16. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 13), dadurch gekennzeichnet, daß der Empfänger (3) eine im Dateneingabegerät (1) eingebauter Funkempfänger ist, welcher die TAN oder das vergleichbare Paßwort auf dem Display oder Monitor des Dateneingabegeräts (1) ausgibt.

17. Vorrichtung nach Anspruch 14), dadurch gekennzeichnet, daß der Funkempfänger ein Benutzer-Identifizierungelement besitzt.

18. Vorrichtung nach Anspruch 15), dadurch gekennzeichnet, daß das Benutzer-Identifizierungelement eine Magnet- oder Chipkarte ist.

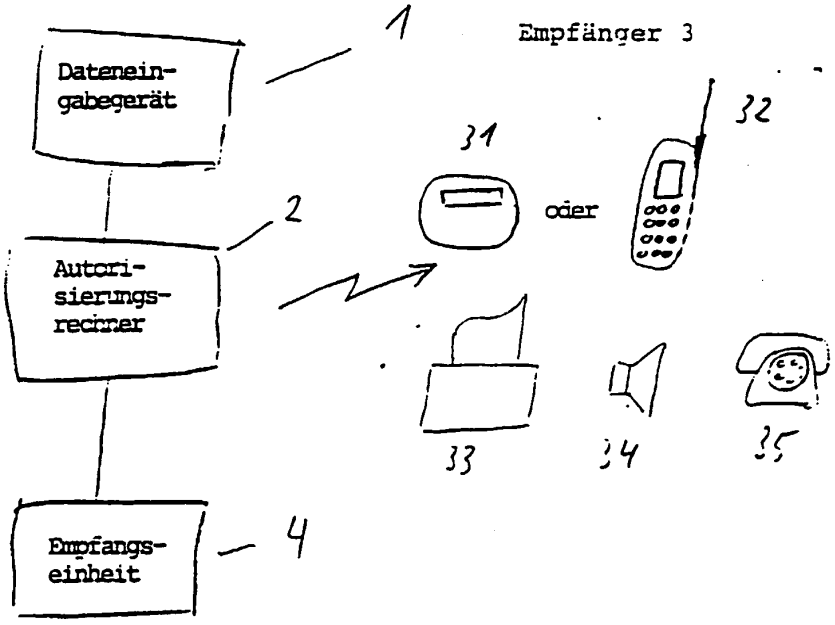
19. Vorrichtung nach Anspruch 15), dadurch gekennzeichnet, daß das Benutzer-Identifizierungelement mit grafischen Einrichtungen zur Überprüfung eines Fingerabdruckes oder zu einer Bildidentifizierung des Benutzers arbeitet.

20. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 17), dadurch gekennzeichnet, daß im Autorisierungsrechner (2) und im Empfänger (3) übereinstimmende Verschlüsselungs-Module vorhanden sind.

21. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 18), dadurch gekennzeichnet, daß die Empfangseinheit (4) ein Türschließ-Mechanismus ist.

22. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 19), dadurch gekennzeichnet, daß der Autorisierungsrechner (2) und die Empfangseinheit (4) in einem Gerät integriert sind.

23. Vorrichtung zur Ausführung des Verfahrens nach einem oder mehreren der Ansprüche 1) bis 19), dadurch gekennzeichnet, daß das Dateneingabegerät, der Autorisierungsrechner (2) und die Empfangseinheit (4) in einem Gerät integriert sind.


1
Empfänger 3
Datenein-
gabegerät
31
32
oder
2
Autori-
sierungs-
rechner
33
34
35
Empfangs-
einheit
4

(staple inside file in blue slip area)

2700 INTERNAL TRANSFER REQUEST FOR S.N. 09/579825

DATE: 8/31/10 FROM: NGuyen (print name)

FORWARD TO:
A. Art Unit: 2785
B. Class: 713
C Subclass: 202

REASON(S):
A. You had Parent [ ] (check box)
B. See Title [X] (check box)
C. See Abstract [ ] (check box)
D. See Claim(s):

FURTHER EXPLANATION IF NEEDED:

DATE: FROM: (print name)

FORWARD TO:
A. Art Unit:
B. Class:
C Subclass:

REASON(S):
A. You had Parent [ ] (check box)
B. See Title [ ] (check box)
C. See Abstract [ ] (check box)
D. See Claim(s):

FURTHER EXPLANATION IF NEEDED:

DATE: FROM: (print name)

FORWARD TO CLASSIFIER

REASON(S):
A. You had Parent [ ] (check box)
B. See Title [ ] (check box)
C. See Abstract [ ] (check box)
D. See Claim(s):

FURTHER EXPLANATION IF NEEDED:

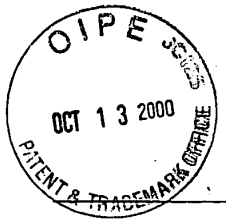
DISPOSITION BY 2700 CLASSIFICATION

DATE: CLASSIFIER:

FORWARD TO:
A. Art Unit:
B. Class:
C Subclass:

REASON(S):
A. You had Parent [ ] (check box)
B. See Title [ ] (check box)
C. See Abstract [ ] (check box)
D. See Claim(s):

FURTHER EXPLANATION IF NEEDED:



RECEIPT

FILE COPY PATENT

Case Docket No. APRILS.001A
Date: October 9, 2000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Engberg, et al.
Appl. No.	:	09/519,829
Filed	:	March 6, 2000
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
Examiner	:	UNKNOWN
Group Art Unit	:	2777

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on

October 9, 2000
(Date)

Alexander Franco, Reg. No. 45,753

RECEIVED
NOV -2 2000
TC 2700 MAIL ROOM

TRANSMITTAL LETTER

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

ATTENTION: OFFICE OF INITIAL PATENT EXAMINATION
CUSTOMER SERVICE CENTER

Dear Sir:

Enclosed for filing in the above-identified application are the following:

(X) A Request for Corrected Filing Receipt;

(X) Copy of Official Filing Receipt with error highlighted in yellow ink; and

(X) A return prepaid postcard.

The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment, to Account No. 11-1410. A duplicate copy of this sheet is enclosed.

Alexander Franco
Registration No. 45,753
Attorney of Record

H:\DOCS\ASF\ASF-1658.DOC\dns
100700

KNOBBE, MARTENS, OLSON & BEAR, LLP
620 NEWPORT CENTER DR 16TH FLOOR NEWPORT BEACH, CA 92660
(949) 760-0404 FAX (949) 760-9502

OIPE JC126 OCT 13 2000 PATENT & TRADEMARK OFFICE

APRILS.001A PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Engberg, et al.	Group Art Unit 2777
Appl. No.	:	09/519,829	
Filed	:	March 6, 2000	
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION	
Examiner	:	UNKNOWN	

RECEIVED NOV -2 2000 TC 2700 MAIL ROOM

REQUEST FOR CORRECTED FILING RECEIPT

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Applicants hereby request that the Official Filing Receipt, a copy of which is enclosed, be corrected to reflect the true title for the above-identified patent application. The title on the receipt currently reads "USE PERSONAL COMMUNICATION DEVICES FOR USERAUTHENTICATION," and should be changed to --USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION--.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 10/9/00

By: _____

Alexander Franco
Registration No. 45,753
Attorney of Record
620 Newport Center Drive, Sixteenth Floor
Newport Beach, CA 92660
(949) 760-0404

H:\DOCS\ASF\ASF-1657.DOC\dns\100700

APRILS.001A
SCJ /ASF

FILING RECEIPT

OC000000005264245

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: ASSISTANT SECRETARY AND
COMMISSIONER OF PATENT AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NUMBER	FILING DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	DRAWINGS	TOT CLAIMS	IND CLAIMS
09/519,829	03/06/2000	2777	614	APRILS.001A	11	27	4

20995
KNOBBE MARTENS OLSON & BEAR LLP
620 NEWPORT CENTER DRIVE
SIXTEENTH FLOOR
NEWPORT BEACH, CA 92660

OIPE JC#226 OCT 13 2000 PATENT & TRADEMARK OFFICE

Date Mailed: 07/24/2000

Receipt is acknowledged of this nonprovisional Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please write to the Office of Initial Patent Examination's Customer Service Center. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the PTO processes the reply to the Notice, the PTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).**

Applicant(s)

Sten-Olov Engberg, Storvreta, SWEDEN;
Ake Jonsson, Fagersta, SWEDEN;

Continuing Data as Claimed by Applicant

Foreign Applications

If Required, Foreign Filing License Granted 04/14/2000

RECEIVED NOV -2 2000 TC 2700 MAIL ROOM

NO DATES DOCKETED ATTY RESPONSIBLE

**** SMALL ENTITY ****

Title

Use personal communication devices for userauthentication

Preliminary Class

713

Data entry by : BURSE, JANICE **Team :** OIPE **Date:** 07/24/2000

FILE COPY

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

Bib Data Sheet

SERIAL NUMBER	FILING DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
09/519,829	03/06/2000 RULE _	713	2777	APRILS.001A

APPLICANTS

Sten-Olov Engberg, Storvreta, SWEDEN;
Ake Jonsson, Fagersta, SWEDEN;

** CONTINUING DATA **********

** FOREIGN APPLICATIONS **********

IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 04/14/2000

** SMALL ENTITY **

Foreign Priority claimed	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ yes ☐ no	SWEDEN	11	27	4

35 USC 119 (a-d) conditions met ☐ yes ☐ no ☐ Met after Allowance

Verified and Acknowledged _____ Examiner's Signature Initials

ADDRESS

20995

TITLE

Use of personal communication devices for user authentication

FILING FEE RECEIVED	
614	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:

☐ All Fees
☐ 1.16 Fees (Filing)
☐ 1.17 Fees (Processing Ext. of time)
☐ 1.18 Fees (Issue)
☐ Other _____
☐ Credit

2177 2777

PATENT

Case Docket No. APRILS.001A
Date: January 8, 2001

RECEIVED
JAN 1 8 2001
Technology Center 2100

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



Applicants	:	Engberg, et al.
Appl. No.	:	09/519,829
Filed	:	March 6, 2000
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
Examiner	:	UNKNOWN
Group Art Unit	:	2777

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on

January 8, 2001
(Date)

Alexander Franco, Reg. No. 45,753

TRANSMITTAL LETTER

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

ATTENTION: APPLICATION BRANCH

Dear Sir:

Enclosed for filing in the above-identified application are the following documents:

(X) A Supplemental Information Disclosure Statement;

(X) A PTO Form 1449 listing one (1) reference, copy of which is enclosed; and

(X) A return prepaid postcard.

The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment, to Account No. 11-1410. A duplicate copy of this sheet is enclosed.

Alexander Franco
Registration No. 45,753
Attorney of Record

H:\DOCS\ASF\ASF-1801.DOC\dns
010801

KNOBBE, MARTENS, OLSON & BEAR, LLP
620 NEWPORT CENTER DR 16TH FLOOR NEWPORT BEACH, CA 92660
(949) 760-0404 FAX (949) 760-9502

APRILS.001A PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

OIPE JC68 JAN 12 2001 PATENT & TRADEMARK OFFICE

RECEIVED
JAN 18 2001
Technology Center 2100

Applicants	:	Engberg, et. al.	Group Art Unit 2777
App. No.	:	09/519,829	
Filed	:	March 6, 2000	
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION	
Examiner	:	UNKNOWN	

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed is form PTO-1449 listing one (1) reference that is also enclosed. This Supplemental Information Disclosure Statement is being filed before the receipt of a first Office Action on the merits, and presumably no fee is required in accordance with 37 C.F.R. § 1.97(b)(3). If a first Office Action on the merits was mailed before the mailing date of this Statement, the Commissioner is authorized to charge the fee set forth in 37 C.F.R. § 1.17(p) to Deposit Account 11-1410. A duplicate copy of this Statement is enclosed for that purpose.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 1/8/01

By: _____

Alexander Franco
Registration No. 45,753
Attorney of Record
620 Newport Center Drive, Sixteenth Floor
Newport Beach, CA 92660
(949) 760-0404

H:\DOCS\ASF\ASF-1799.DOC\dns\010801

OIPE JC175 MAR 1 2 2001 PATENT & TRADEMARK OFFICE

2177 2200

PATENT

Case Docket No. APRILS.001A
Date: March 7, 2001
Page 1

In re application of	:	Engberg, et al.
App. No.	:	09/519,829
Filed	:	March 6, 2000
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
Examiner	:	UNKNOWN
Art Unit	:	2777

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on

March 7, 2001
(Date)

Alexander Franco, Reg. No. 45,753

RECEIVED MAR 14 2001 Group 2100

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

Sir:

Transmitted herewith is a preliminary amendment in the above-identified application.

The fee has been calculated as shown below:

CLAIMS AS FILED

	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NO. PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDITIONAL FEE
Total Claims	26	—	27	= 0 ×	$9	= $ 0
Independent Claims	5	—	4	= 1 ×	$40	= $40.00
If application has been amended to contain multiple dependent claim(s), then add					$135	= $ 0
Time Extension Fee						$ 0
				TOTAL ADDITIONAL FEE FOR THIS AMENDMENT		$40.00

Assignee is a small entity and such status is proper and desired.

Enclosed with the preliminary amendment are the following:

(X) A check in the amount of $40.00; and
(X) A return prepaid postcard.

KNOBBE, MARTENS, OLSON & BEAR, LLP
620 NEWPORT CENTER DR 16TH FLOOR NEWPORT BEACH, CA 92660
(949) 760-0404 FAX (949) 760-9502

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410. A duplicate copy of this sheet is enclosed.

Alexander Franco
Registration No. 45,753
Attorney of Record

H:\DOCS\ASF\ASF-1963.DOC\dns
030701

KNOBBE, MARTENS, OLSON & BEAR, LLP
620 NEWPORT CENTER DR 16TH FLOOR NEWPORT BEACH, CA 92660
(949) 760-0404 FAX (949) 760-9502

OIPE
MAR 1 2 2001
PATENT & TRADEMARK OFFICE

7/C
3/21/01
Roy

APRILS.001A

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Engberg, et. al.	Group Art Unit 2777
App. No.	:	09/519,829	
Filed	:	March 6, 2000	
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION	
Examiner	:	UNKNOWN	

RECEIVED
MAR 1 4 2001
Group 2100

03/13/2001 RHARIS1 00000135 09519829
01 FC:202 40.00 OP

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Prior to examination on the merits, please amend the above-referenced application as indicated below.

In the Specification:

Please replace the paragraph beginning on page 1, line 7 of the Specification with the following rewritten paragraph:

a1

This invention relates generally to the authentication of users of secure systems and, more particularly, the invention relates to a system through which user tokens required for user authentication are supplied through personal communication devices such as mobile telephones and pagers.

Please replace the paragraph beginning on page 5, line 22 of the Specification with the following rewritten paragraph:

a2

Figure 1 illustrates an overview, including system components, of a user authentication system 100 according to a preferred embodiment of the present invention. Figure 2A illustrates a

login screen that can be used in accordance with the preferred embodiment. Figures 2B-D illustrate login screens that can be used in accordance with alternative embodiments.--

In the Claims:

Please cancel Claims 1-27 without prejudice and add the following new claims:

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.

29. The method of Claim 28, wherein the new password is generated by concatenating the token and the passcode.

30. The method of Claim 28, further comprising receiving a request from the user for the token.

31. The method of Claim 30, wherein the request is transmitted by the user through the personal communication device.

32. The method of Claim 28, wherein the personal communication device is a mobile phone.

33. The method of Claim 28, wherein the personal communication device is a pager.

34. A user authentication system comprising:

a user database configured to associate a user with a personal communication device possessed by the user;

a control module 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;

a communication module configured to transmit the token to the personal communication device; and

an authentication module configured to receive the password from the user.

35. The system of Claim 34, 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.

36. The system of Claim 35, wherein the request is transmitted by the user through the personal communication device.

37. A method of regulating access to a secure system, the method comprising:

associating the user with a personal communication device possessed by the user;

associating the user with an account, wherein an initiation of access through the account requires that the account be activated;

receiving a request transmitted by the personal communication device; and

in response to the receipt of the request, activating the account.

38. The method of Claim 37, further comprising deactivating the account within a predetermined amount of time after the account is activated.

39. The method of Claim 37, wherein an initiation of access through the account further requires that the user supply a valid password.

40. The method of Claim 39, further comprising:

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 the valid password to be the new password;

transmitting the token to the personal communication device; and

receiving the valid password from the user.

41. The method of Claim 40, wherein the new password is generated by concatenating the token and the passcode.

42. The method of Claim 40, wherein the token is transmitted in response to the receipt of the request.

43. A method of regulating access to a secure system, the method comprising:

receiving a request for a token, wherein the request is transmitted from a personal communication device as a result of an action by a user;

in response to the receipt of the request, transmitting the token to the personal communication device;

receiving login data from the user in response to a request for authentication information, wherein the login data is based at least upon the token; and

granting access to the secure system based at least upon the received login data.

44. The method of Claim 43, wherein the login data is additionally based upon a passcode known to the user.

45. The method of Claim 43, wherein the login data comprises a password.

46. The method of Claim 45, wherein the password comprises a passcode and the token, and wherein the passcode is known to the user.

47. The method of Claim 46, wherein the password is a concatenation of the passcode and the token.

48. The method of Claim 46, wherein the password is a hashed concatenation of the passcode and the token.

49. The method of Claim 43, further comprising generating the token.

50. An access control system comprising:

a communication module configured to receive a request for a token, wherein the request is transmitted from a personal communication device as a result of an action by a user, and wherein the communication module is further configured to transmit the token to the personal communication device in response to the request;

a user token server configured to generate a valid password based at least upon the token; and

an authentication module configured to receive a submitted password in response to a request for authentication of the user, the authentication module further configured to grant access to the user if at least the submitted password matches the valid password.

51. The system of Claim 50, wherein the user token server is further configured to generate the valid password based additionally upon a passcode that is known to the user.

52. The system of Claim 51, wherein the valid password is a concatenation of the passcode and the token.

53. The system of Claim 50, wherein the user token server is further configured to generate the token.

REMARKS

The Specification has been amended to correct a number of minor clerical errors.

Claims 1-27 have been replaced with Claims 28-53, which are supported by the originally filed specification.

Marked-up versions of the changes to the Specification have been attached at the end of this document.

If any issues arise during the examination of this application, the Examiner is invited to call the undersigned applicant at 949-721-3677.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 3/7/01

By: _____

Alexander Franco
Registration No. 45,753
Attorney of Record
620 Newport Center Drive, Sixteenth Floor
Newport Beach, CA 92660
(949) 760-0404

H:\DOCS\ASF\ASF-1959.DOC
030601

OIPE JC175 MAR 12 2001 PATENT & TRADEMARK OFFICE

MARKED UP VERSIONS OF AMENDMENTS TO THE APPLICATION

Marked up version of the paragraph beginning on page 1, line 7 of the Specification:

-- This invention relates generally to the authentication of users of secure systems and, more particularly, the invention relates to a system through which user tokens required for user authentication are supplied through personal communication devices such as mobile telephones and pagers.--

Marked up version of the paragraph beginning on page 5, line 22 of the Specification:

-- Figure 1 illustrates an overview, including system components, of a user authentication system 100 according to a preferred embodiment of the present invention. Figure 2A illustrates a login screen that can be used in accordance with the preferred embodiment. Figures 2B-D illustrate ~~a~~ login screens that can be used in accordance with alternative embodiments.--

H:\DOCS\ASF\ASF-1962.DOC
030601

2131

PATENT

Case Docket No. APRILS.001A
Date: March 7, 2001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Engberg, et al.
Appl. No.	:	09/519,829
Filed	:	March 6, 2000
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
Group Art Unit	:	2777
Batch No.	:	UNKNOWN
Examiner	:	UNKNOWN

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on

March 7, 2001
(Date)

Alexander Franco, Reg. No. 45,753

OIPE JC106 MAR 12 2001 PATENT & TRADEMARK OFFICE

RECEIVED
MAR 14 2001
Group 2100

TRANSMITTAL LETTER

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

ATTENTION: OFFICIAL DRAFTSPERSON

Dear Sir:

Enclosed for filing are 11 sheets of formal drawings and a return prepaid postcard.

The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment, to Account No. 11-1410. A duplicate copy of this sheet is enclosed.

Alexander Franco
Registration No. 45,753
Attorney of Record

H:\DOCS\ASF\ASF-1964.DOC\dns
030701

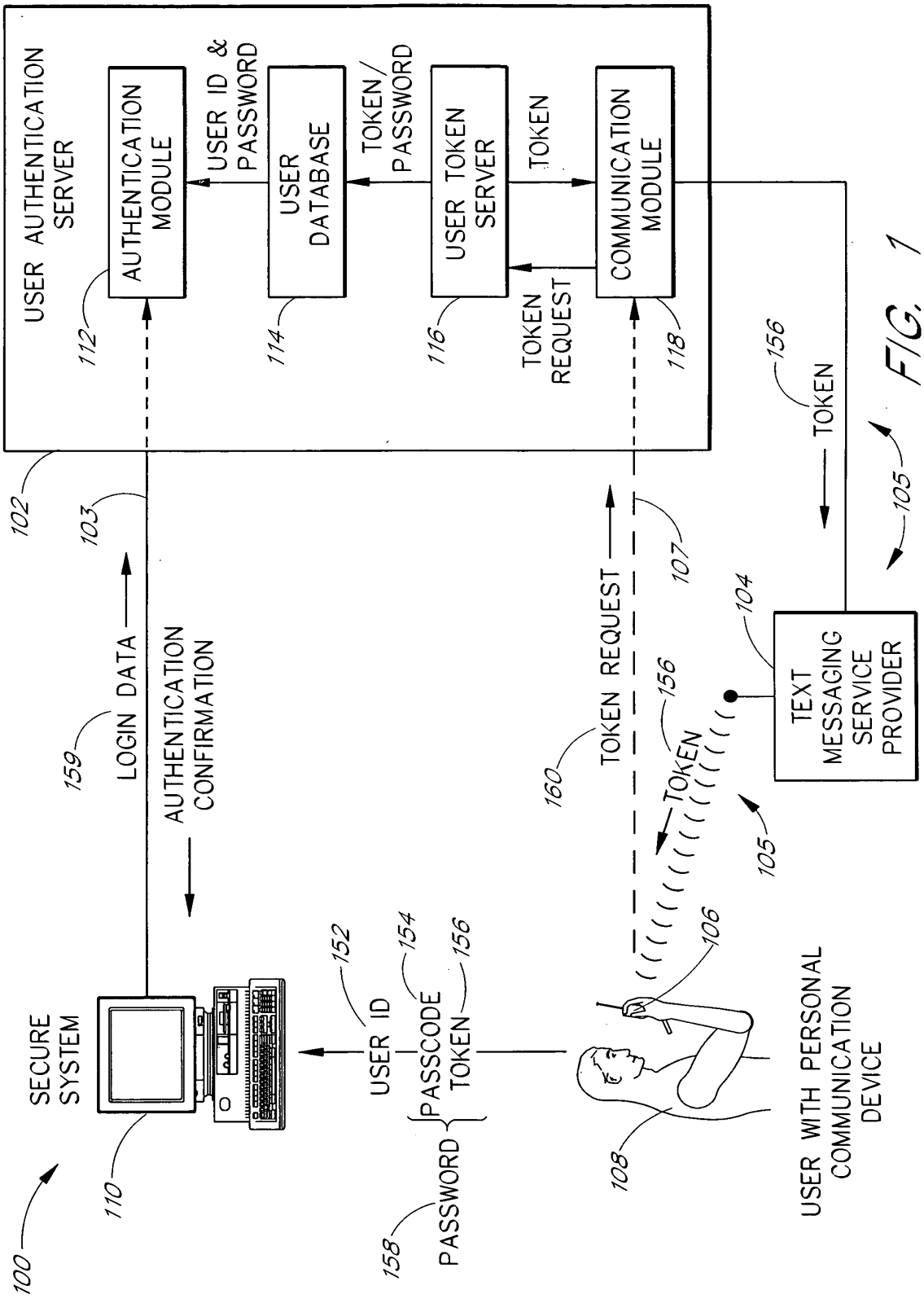

USER AUTHENTICATION SERVER
AUTHENTICATION MODULE
USER ID & PASSWORD
USER DATABASE
TOKEN / PASSWORD
USER TOKEN SERVER
TOKEN
COMMUNICATION MODULE
TOKEN REQUEST
112
114
116
118
102
103
107
105
156
TOKEN
LOGIN DATA
159
AUTHENTICATION CONFIRMATION
TOKEN REQUEST
160
TOKEN
156
104
TEXT MESSAGING SERVICE PROVIDER
105
SECURE SYSTEM
110
100
152
154
156
USER ID
PASSCODE
TOKEN
PASSWORD
158
106
108
USER WITH PERSONAL COMMUNICATION DEVICE

FIG. 1

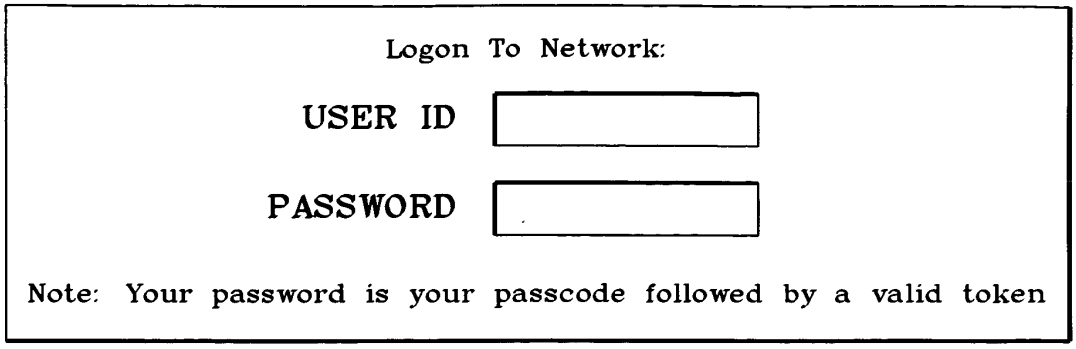


FIG. 2A

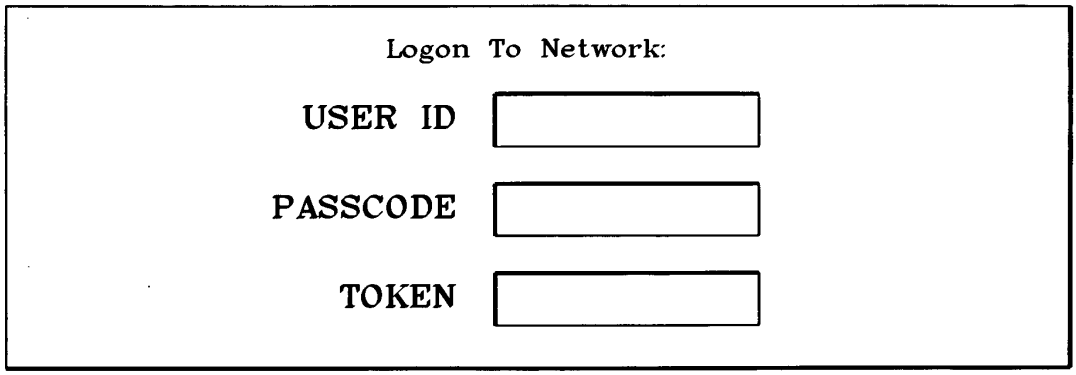


FIG. 2B

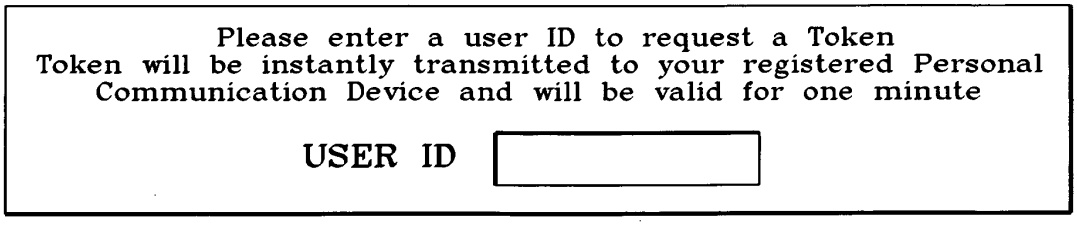


FIG. 2C

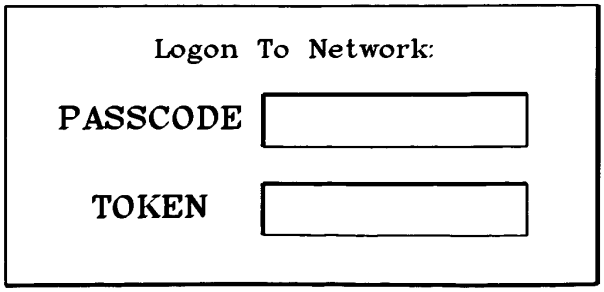


FIG. 2D

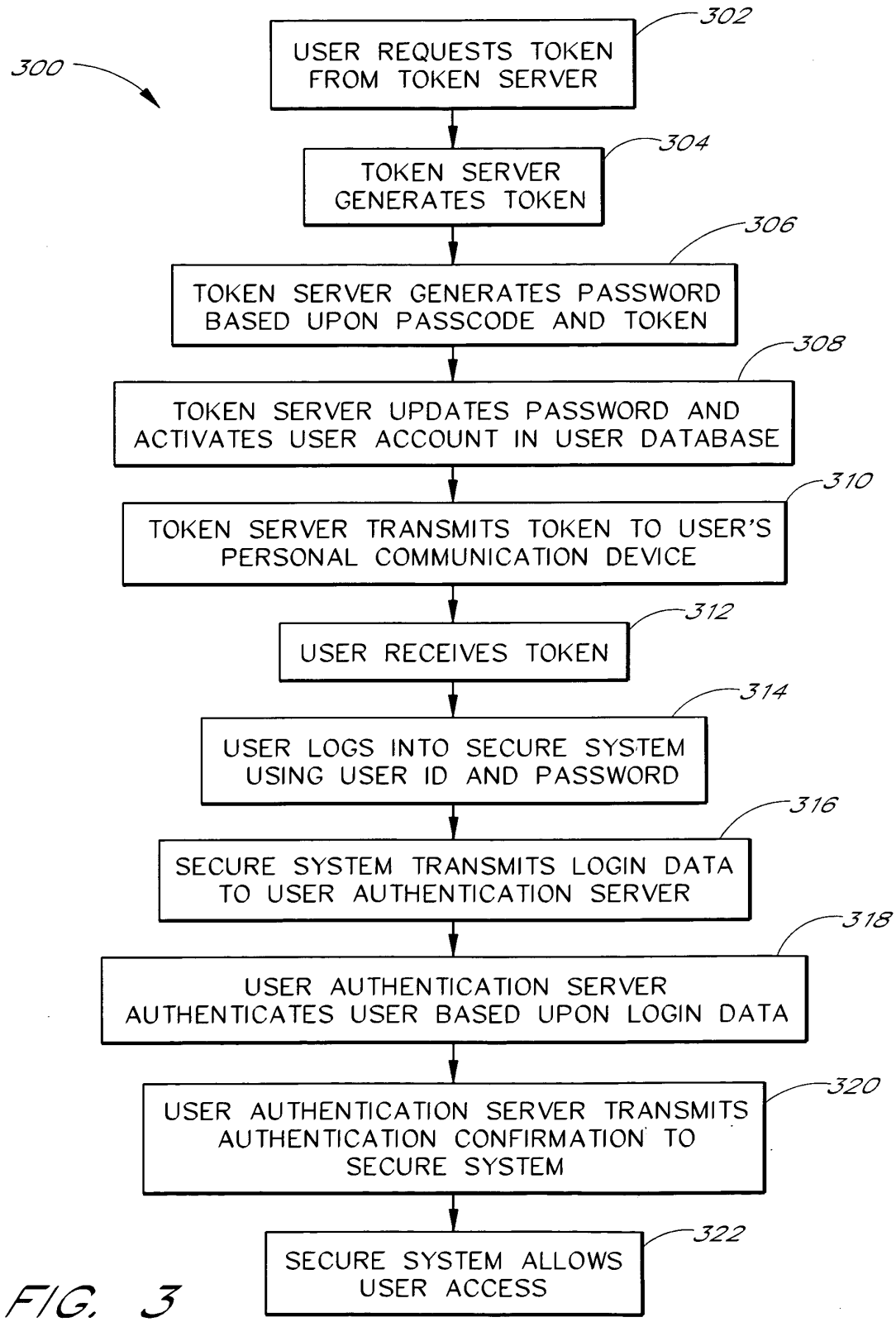

300
USER REQUESTS TOKEN FROM TOKEN SERVER
302
TOKEN SERVER GENERATES TOKEN
304
TOKEN SERVER GENERATES PASSWORD BASED UPON PASSCODE AND TOKEN
306
TOKEN SERVER UPDATES PASSWORD AND ACTIVATES USER ACCOUNT IN USER DATABASE
308
TOKEN SERVER TRANSMITS TOKEN TO USER'S PERSONAL COMMUNICATION DEVICE
310
USER RECEIVES TOKEN
312
USER LOGS INTO SECURE SYSTEM USING USER ID AND PASSWORD
314
SECURE SYSTEM TRANSMITS LOGIN DATA TO USER AUTHENTICATION SERVER
316
USER AUTHENTICATION SERVER AUTHENTICATES USER BASED UPON LOGIN DATA
318
USER AUTHENTICATION SERVER TRANSMITS AUTHENTICATION CONFIRMATION TO SECURE SYSTEM
320
SECURE SYSTEM ALLOWS USER ACCESS
322

FIG. 3

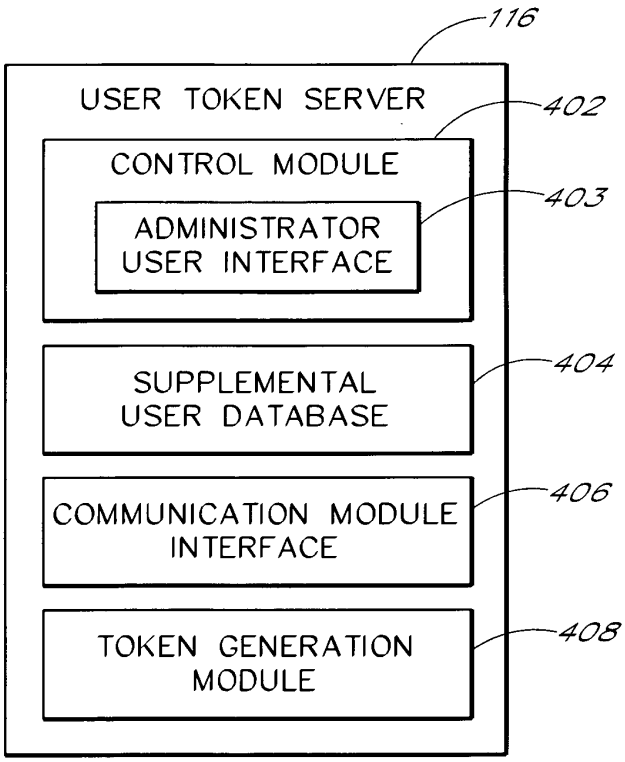

116
USER TOKEN SERVER
402
CONTROL MODULE
403
ADMINISTRATOR USER INTERFACE
404
SUPPLEMENTAL USER DATABASE
406
COMMUNICATION MODULE INTERFACE
408
TOKEN GENERATION MODULE

FIG. 4

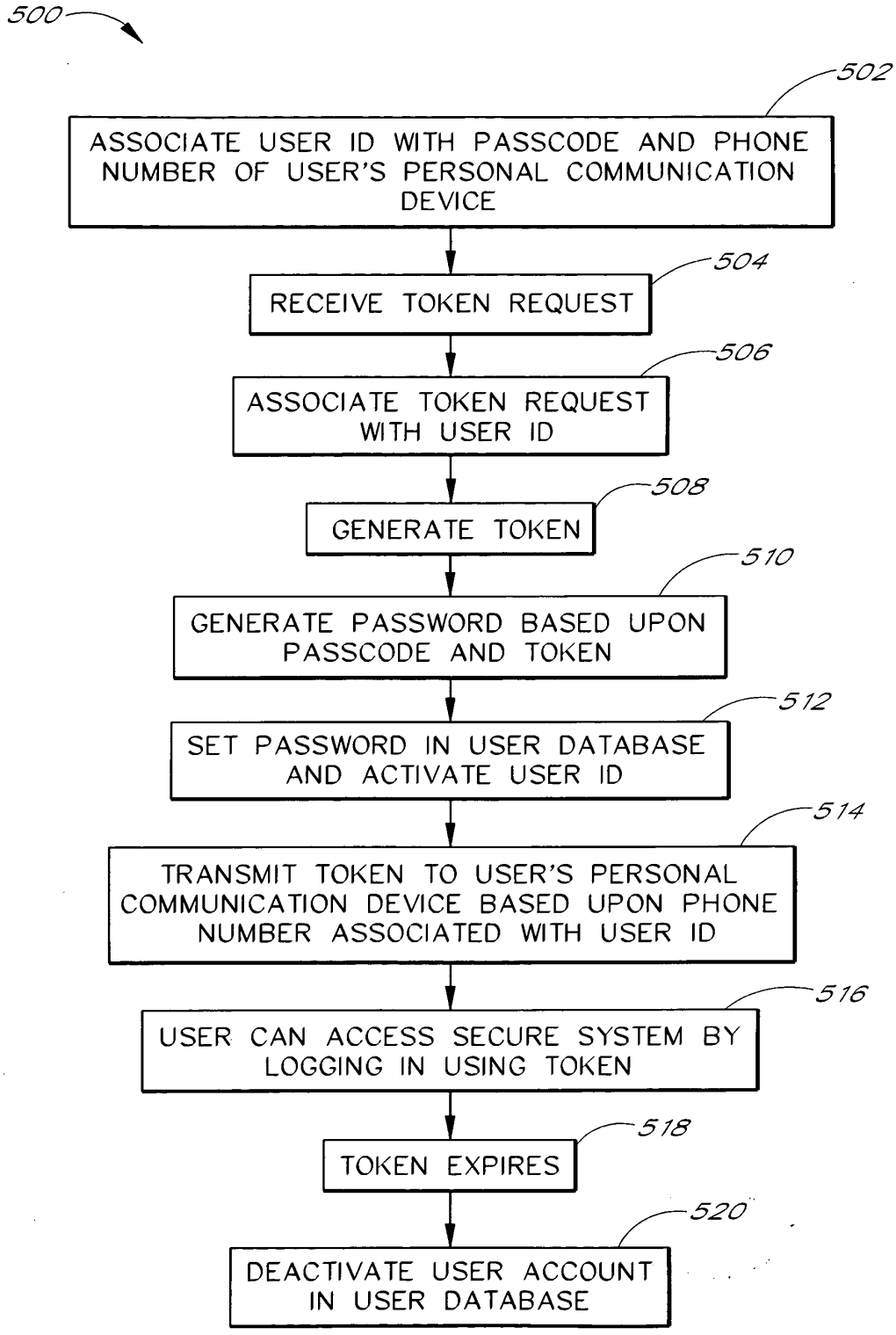

500
502
ASSOCIATE USER ID WITH PASSCODE AND PHONE NUMBER OF USER'S PERSONAL COMMUNICATION DEVICE
504
RECEIVE TOKEN REQUEST
506
ASSOCIATE TOKEN REQUEST WITH USER ID
508
GENERATE TOKEN
510
GENERATE PASSWORD BASED UPON PASSCODE AND TOKEN
512
SET PASSWORD IN USER DATABASE AND ACTIVATE USER ID
514
TRANSMIT TOKEN TO USER'S PERSONAL COMMUNICATION DEVICE BASED UPON PHONE NUMBER ASSOCIATED WITH USER ID
516
USER CAN ACCESS SECURE SYSTEM BY LOGGING IN USING TOKEN
518
TOKEN EXPIRES
520
DEACTIVATE USER ACCOUNT IN USER DATABASE

FIG. 5

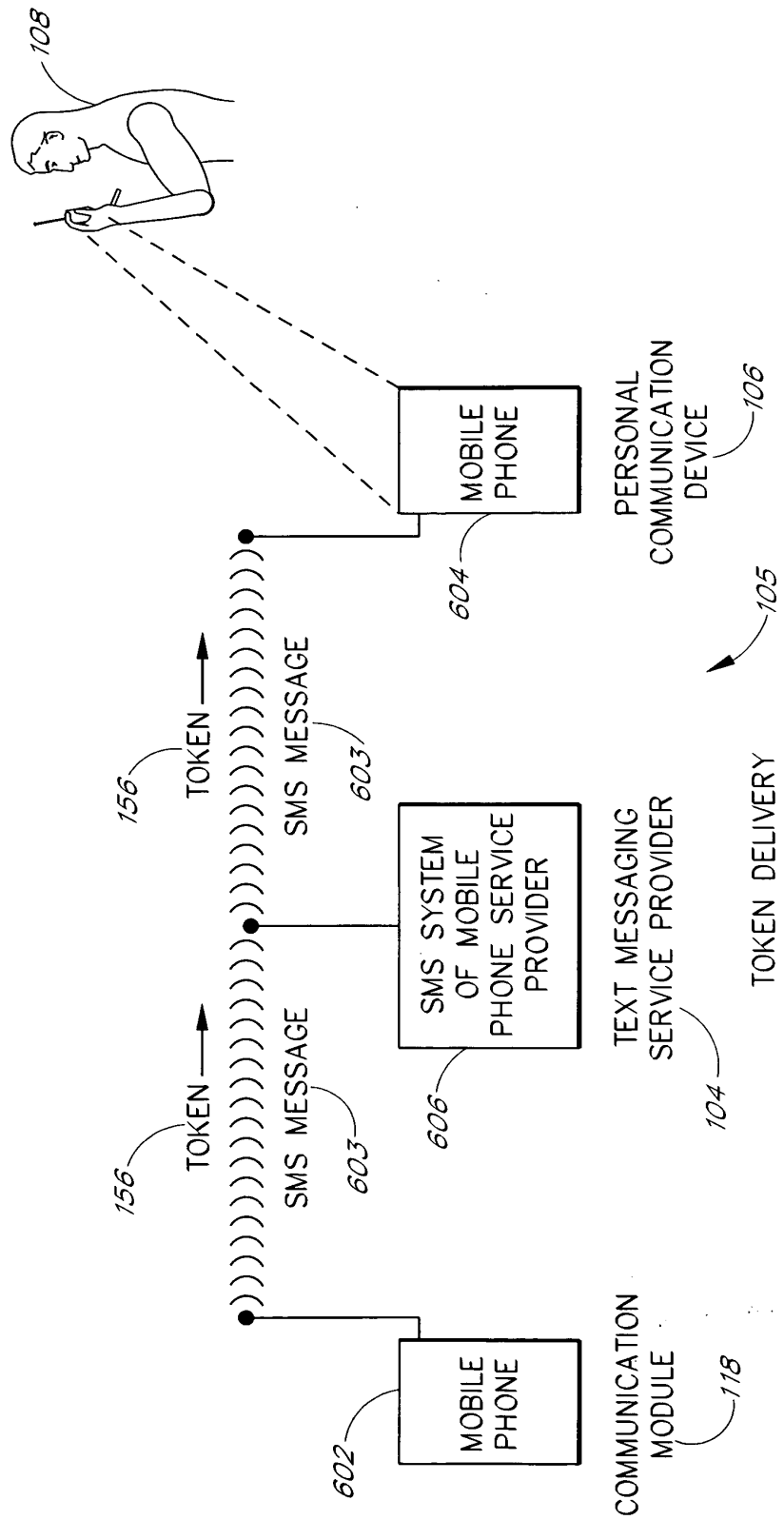

108
MOBILE PHONE
604
PERSONAL COMMUNICATION DEVICE
106
105
TOKEN
156
SMS MESSAGE
603
SMS SYSTEM OF MOBILE PHONE SERVICE PROVIDER
606
TEXT MESSAGING SERVICE PROVIDER
104
TOKEN DELIVERY
TOKEN
156
SMS MESSAGE
603
MOBILE PHONE
602
COMMUNICATION MODULE
118

FIG. 6A

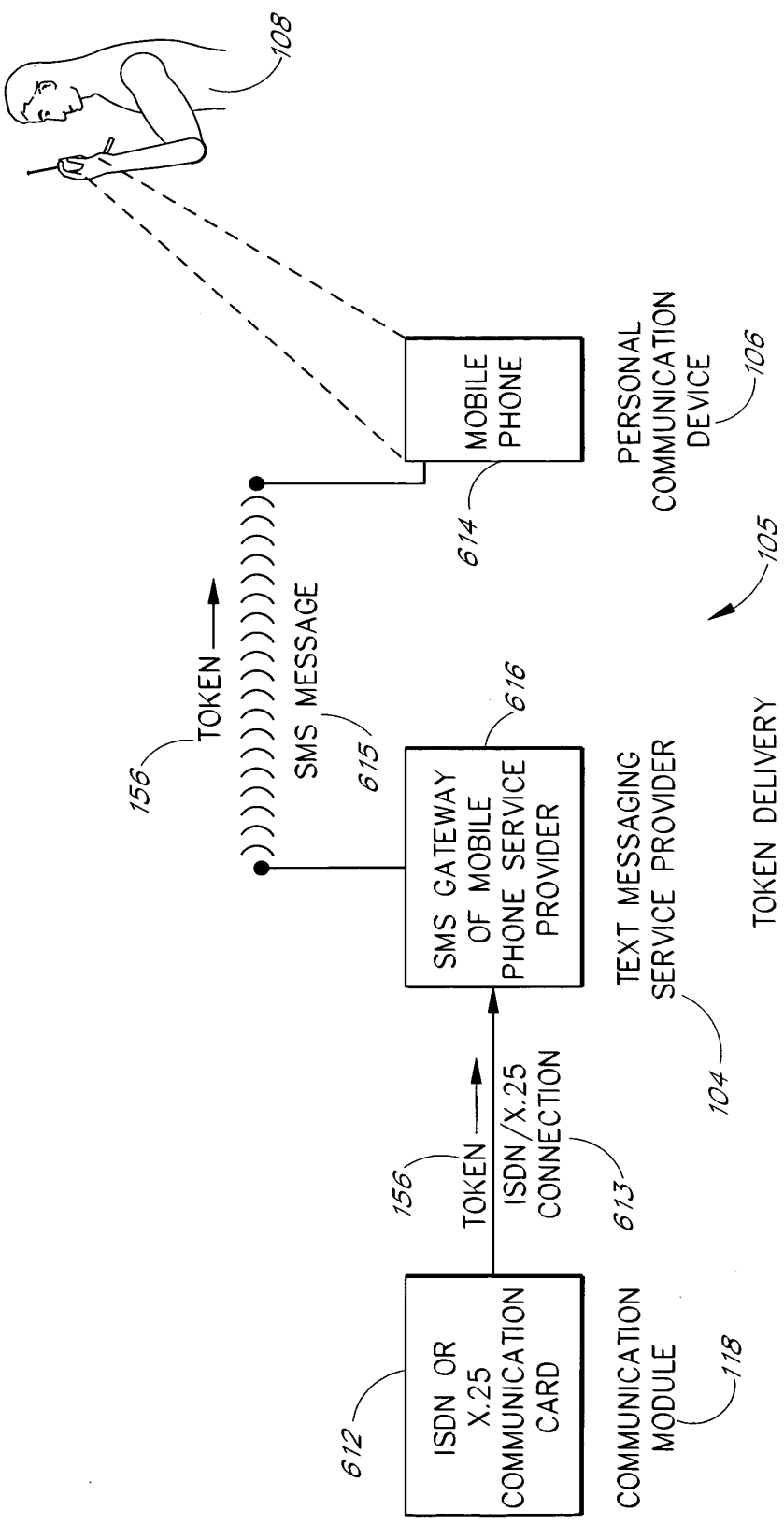

108
MOBILE PHONE
614
PERSONAL COMMUNICATION DEVICE
106
105
TOKEN
156
SMS MESSAGE
615
SMS GATEWAY OF MOBILE PHONE SERVICE PROVIDER
616
TEXT MESSAGING SERVICE PROVIDER
104
TOKEN DELIVERY
TOKEN
156
ISDN/X.25 CONNECTION
613
ISDN OR X.25 COMMUNICATION CARD
612
COMMUNICATION MODULE
118

FIG. 6B

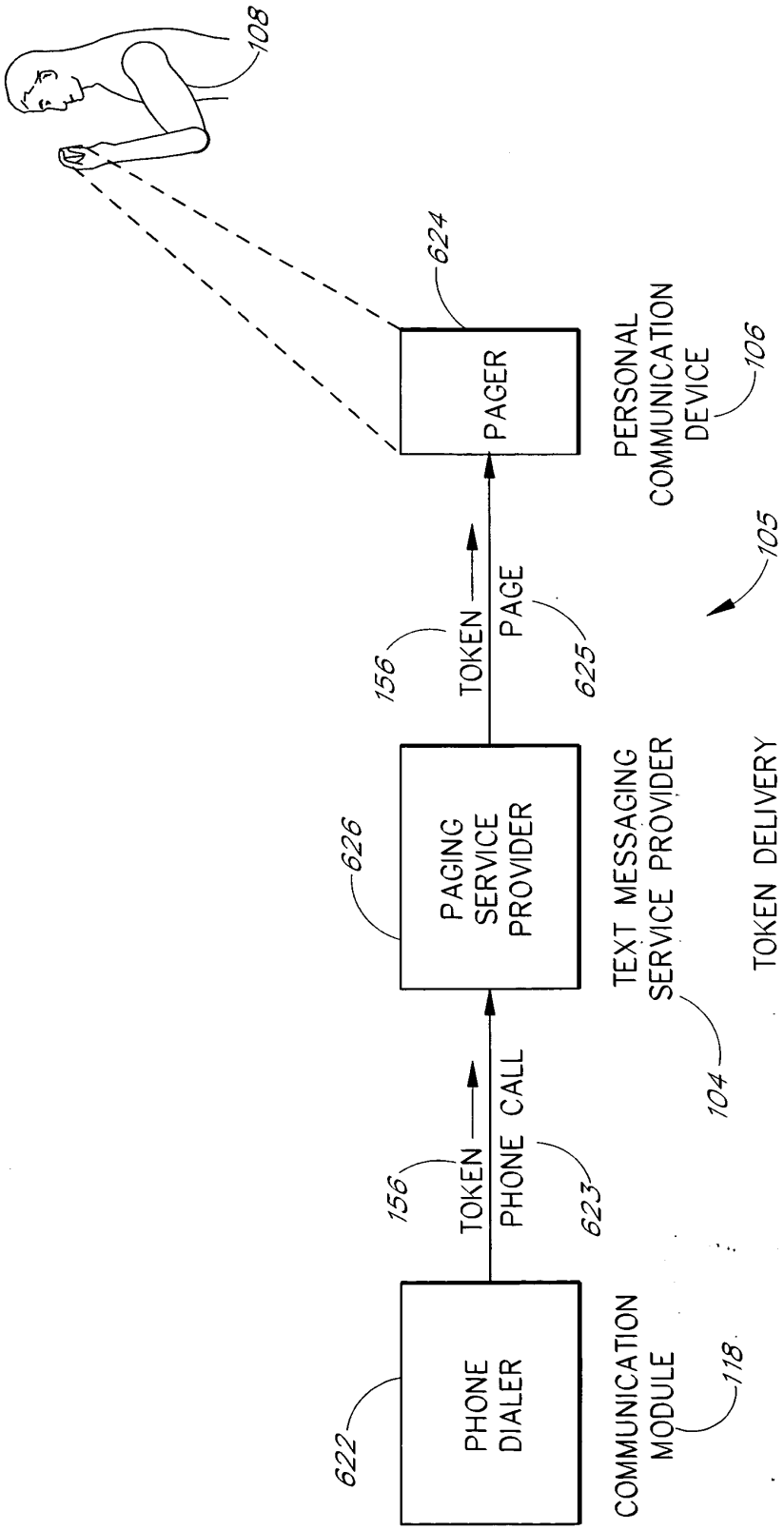

108
624
PAGER
PERSONAL COMMUNICATION DEVICE
106
105
156
TOKEN
PAGE
625
626
PAGING SERVICE PROVIDER
TEXT MESSAGING SERVICE PROVIDER
104
TOKEN DELIVERY
156
TOKEN
PHONE CALL
623
622
PHONE DIALER
COMMUNICATION MODULE
118

FIG. 6C

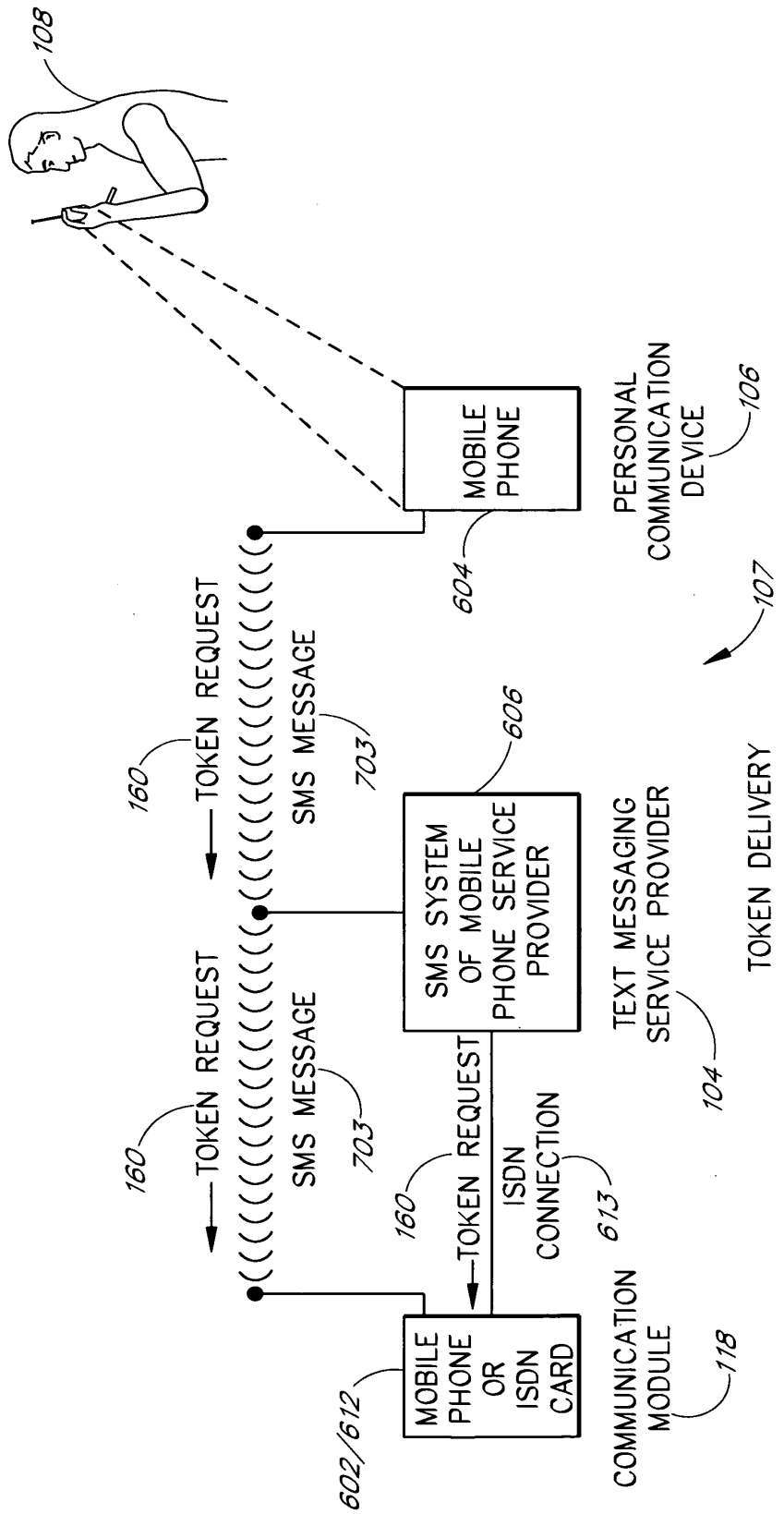

108
MOBILE PHONE
604
PERSONAL COMMUNICATION DEVICE
106
107
TOKEN DELIVERY
160
TOKEN REQUEST
SMS MESSAGE
703
606
SMS SYSTEM OF MOBILE PHONE SERVICE PROVIDER
TEXT MESSAGING SERVICE PROVIDER
104
160
TOKEN REQUEST
SMS MESSAGE
703
160
TOKEN REQUEST
ISDN CONNECTION
613
MOBILE PHONE OR ISDN CARD
602/612
COMMUNICATION MODULE
118

FIG. 7A

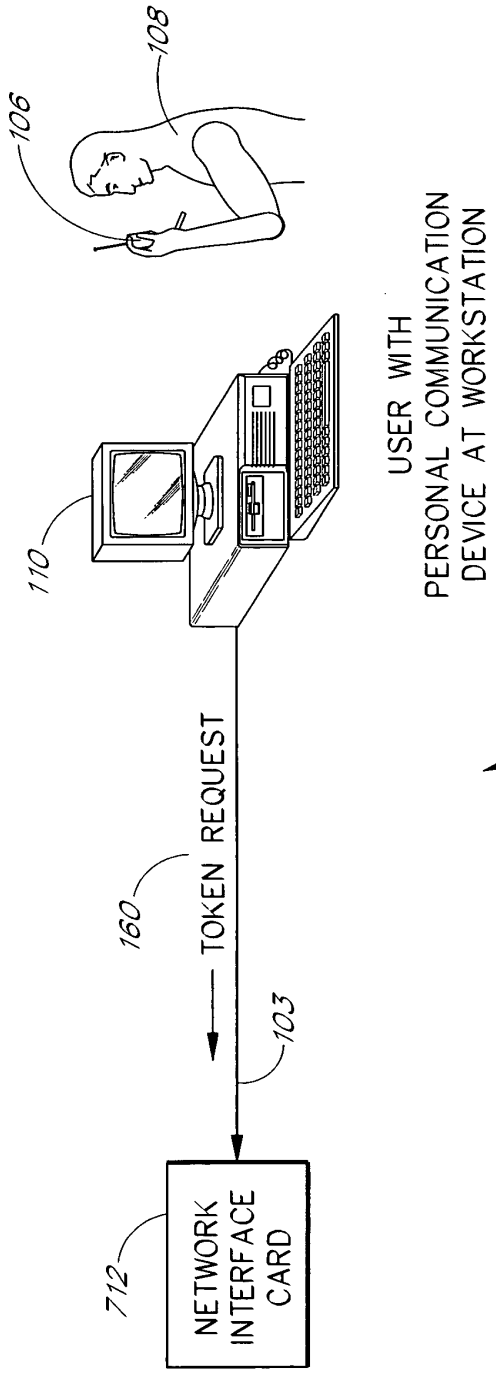

106
108
USER WITH
PERSONAL COMMUNICATION
DEVICE AT WORKSTATION
110
TOKEN REQUEST
160
103
NETWORK
INTERFACE
CARD
712
107
TOKEN REQUEST

FIG. 7B

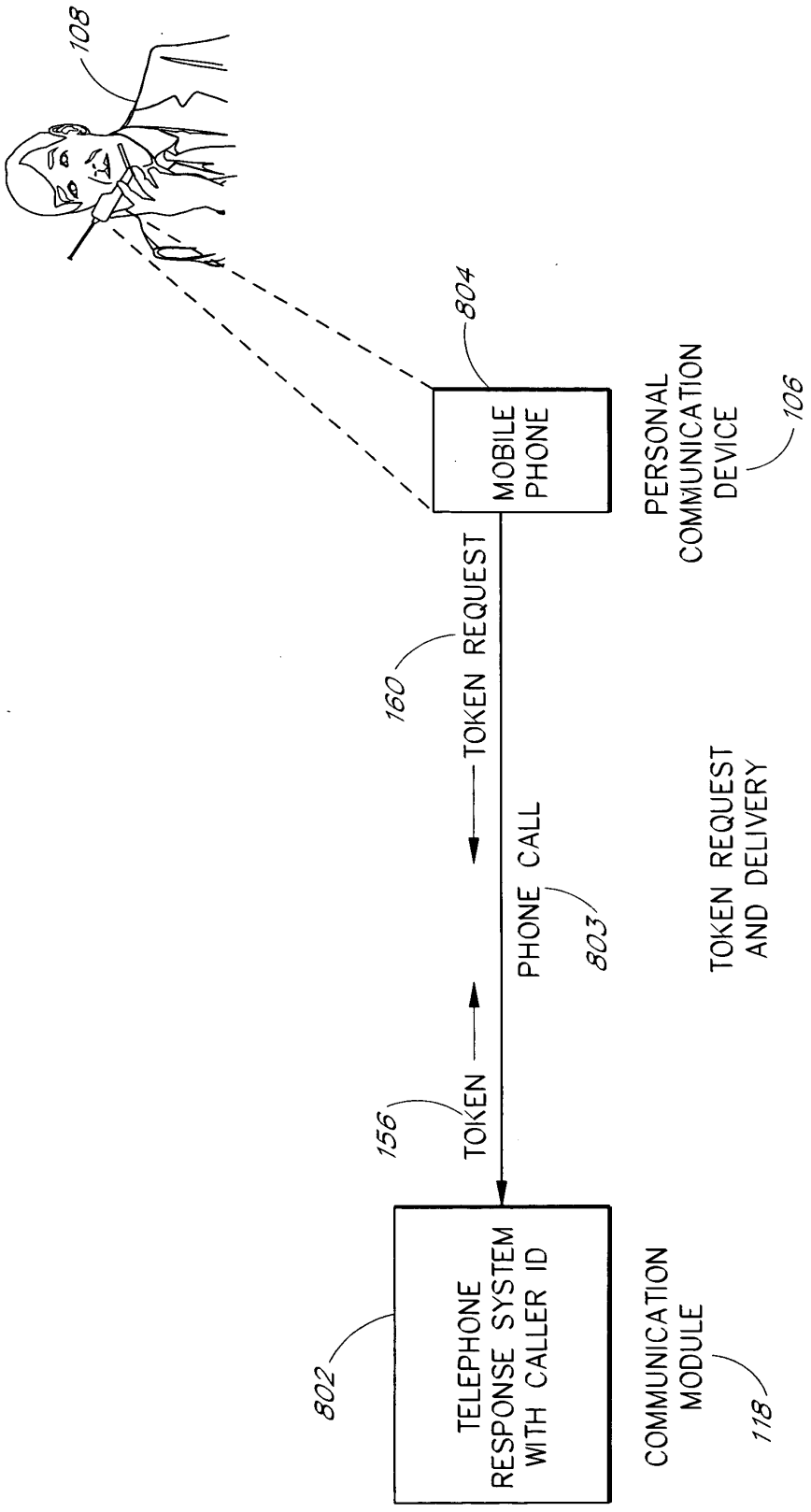

108
804
MOBILE PHONE
PERSONAL COMMUNICATION DEVICE
106
160
TOKEN REQUEST
PHONE CALL
803
TOKEN REQUEST AND DELIVERY
156
TOKEN
802
TELEPHONE RESPONSE SYSTEM WITH CALLER ID
COMMUNICATION MODULE
118

FIG. 8

PATENT & TRADEMARK OFFICE
AUG 09 2001
PTO/SB/34

#9

APRILS.001A

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Engberg, et. al.	Group Art Unit 2777
App. No.	:	09/519,829	
Filed	:	March 6, 2000	
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION	
Examiner	:	UNKNOWN	

RECEIVED
AUG 13 2001
Technology Center 2100

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed is form PTO-1449 listing six (6) references that are also enclosed. The references consist of an International Search Report in corresponding PCT application (no. PCT/US01/07058). This Supplemental Information Disclosure Statement is being filed before the mailing date of a final action under 37 C.F.R. § 1.113 and before the mailing date of a Notice of Allowance under § 1.311. A certification under 37 C.F.R. § 1.97(e) is set forth below. Thus, no fee is required as set forth below in 37 C.F.R. § 1.97(c).

CERTIFICATION UNDER 37 C.F.R. § 1.97(e)(1)

I hereby certify that each item of information contained in this Statement was first cited in a communication from a foreign Patent Office in a counterpart foreign application not more than three months prior to the filing of this Supplemental Information Disclosure Statement.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 8/6/01

By: _____

Alexander Franco, Attorney of Record
Registration No. 45,753
620 Newport Center Drive, Sixteenth Floor
Newport Beach, CA 92660
(949) 760-0404

H:\DOCS\ASF\ASF-2341.DOC\dns\080301

PATENT & TRADEMARK OFFICE
AUG 0 9 2001
JC34
OIPE

GAU 2777
2177
#9

PATENT

Case Docket No. APRILS.001A
Date: August 6, 2001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Engberg, et al.
Appl. No.	:	09/519,829
Filed	:	March 6, 2000
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
Examiner	:	UNKNOWN
Group Art Unit	:	2777

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on

August 6, 2001
(Date)

Alexander Franco, Reg. No. 45,753

RECEIVED
AUG 1 3 2001
Technology Center 2100

TRANSMITTAL LETTER

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

ATTENTION: APPLICATION BRANCH

Dear Sir:

Enclosed for filing in the above-identified application are the following documents:

(X) A Supplemental Information Disclosure Statement;

(X) A PTO Form 1449 listing six (6) references, copies of which are enclosed; and

(X) A return prepaid postcard.

The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment, to Account No. 11-1410. A duplicate copy of this sheet is enclosed.

Alexander Franco
Registration No. 45,753
Attorney of Record

H:\DOCS\ASF\ASF-2343.DOC\dns
080301

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference APRILS.001VP	FOR FURTHER ACTION	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
International application No. PCT/US01/07058	International filing date *(day/month/year)* 06 MARCH 2001	(Earliest) Priority Date *(day/month/year)* 06 MARCH 2000
Applicant APRIL SYSTEM DESIGN, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
   [ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).
   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing:
   [ ] contained in the international application in written form.
   [ ] filed together with the international application in computer readable form.
   [ ] furnished subsequently to this Authority in written form.
   [ ] furnished subsequently to this Authority in computer readable form.
   [ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   [ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has b een furnished.
2. [ ] **Certain claims were found unsearchable** (See Box I).
3. [ ] **Unity of invention is lacking** (See Box II).
4. With regard to the **title**,
   [X] the text is approved as submitted by the applicant.
   [ ] the text has been established by this Authority to read as follows:
5. With regard to the **abstract**,
   [X] the text is approved as submitted by the applicant.
   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.
6. The figure of the **drawings** to be published with the abstract is Figure No. 1
   [X] as suggested by the applicant.
   [ ] because the applicant failed to suggest a figure.
   [ ] because this figure better characterizes the invention.
   [ ] None of the figures.

Form PCT/ISA/210 (first sheet) (July 1998) ★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/07058

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :G06F 1/26
US CL :380/255; 713/150, 155, 159, 168, 172, 182, 185
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/255; 713/150, 155, 159, 168, 172, 182, 185

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, P	US 6,173,400 B1 (PERLMAN et al.), 09 January 2001, col. 11-12, lines 8-67.	7-8
Y	US 6,161,182 A (NADOOSHAN) 12 December 2000, col. 4-8, lines 1-61.	1, 3-4, 9, 10-13, 15-19, 22-23, and 26
Y	US 6,173,400 B1 (PERLMANN et al) 09 January 2001, col. 10-12, lines 1-65.	1, 3-4, 9, 10-13, 15-19, 22-23, and 26
A	US 5,923,763 A (WALKER et al) 13 July 1999, col. 13, lines 1-67.	1-26
A	US 5,590,198 A (LEE et al) 31 December 1996, col. 1-7, lines 1-67.	1-26

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
23 MAY 2001

Date of mailing of the international search report
18 JUN 2001

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
TOD SWANN
Telephone No. (703) 308-7791

Form PCT/ISA/210 (second sheet) (July 1998) ★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/07058

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,049,877 (WHITE) 11 April 2000, col. 8, lines 1-67.	1-26

Form PCT/ISA/210 (continuation of second sheet) (July 1998) ★

L Number	Hits	Search Text	DB	Time stamp
1	567	455/411.ccls. 380/247,249.ccls.	USPAT	2003/12/03 15:12
2	724	(455/411.ccls. 380/247,249.ccls.) and @ad<20000306	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/03 15:54
3	98	((455/411.ccls. 380/247,249.ccls.) and @ad<20000306) and ((pass adj word) password)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/03 15:14

L Number	Hits	Search Text	DB	Time stamp
1	144	(713/$.ccls. 380/$.ccls.) and (((cell cellular) adj phone) pager) and (password (pass adj word))	USPAT	2003/12/04 17:13
2	19	(713/$.ccls. 380/$.ccls.) and ((((cell cellular) adj phone) pager) same (password (pass adj word)))	USPAT	2003/12/04 17:13
3	62	(705/$.ccls. 340/$.ccls.) and ((((cell cellular) adj phone) pager) same (password (pass adj word)))	USPAT	2003/12/04 17:13
4	73	(705/$.ccls. 340/$.ccls. 713/$.ccls. 380/$.ccls.) and ((((cell cellular) adj phone) pager) same (password (pass adj word)))	USPAT	2003/12/04 17:13
6	5	(705/$.ccls. 340/$.ccls. 713/$.ccls. 380/$.ccls.) and ((((cell cellular) adj phone) pager mobile) and ((password (pass adj word)) same seed))	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/04 17:14
5	5	(705/$.ccls. 340/$.ccls. 713/$.ccls. 380/$.ccls.) and ((((cell cellular) adj phone) pager mobile) and ((password (pass adj word)) same seed))	USPAT	2003/12/04 17:14
7	1	(705/$.ccls. 340/$.ccls. 713/$.ccls. 380/$.ccls.) and ((((cell cellular) adj phone) pager) same (password (pass adj word)))	EPO; JPO; DERWENT; IBM_TDB	2003/12/04 17:14
8	12	713/201,202.ccls. and (cell phone pager mobile) and ((concaten$ appen$) same (password (pass adj (code word))))	USPAT	2003/12/04 17:14
10	163	(713/202.ccls. 709/224-229.ccls. 455.411.ccls. 380/247,249.ccls. 340/$.ccls.) and ((concaten$ appen$ certificate) same (password (pass adj (code word))))	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/04 17:14
9	85	(713/202.ccls. 709/224-229.ccls. 455.411.ccls. 380/247,249.ccls. 340/$.ccls.) and ((concaten$ appen$) same (password (pass adj (code word))))	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/04 17:14
11	103	(713/202.ccls. 709/224-229.ccls. 455.411.ccls. 380/247,249.ccls. 340/$.ccls.) and ((concaten$ appen$ certificate) same (password (pass adj (code word))) same user)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/04 17:14
12	55	(713/202.ccls. 709/224-229.ccls. 455.411.ccls. 380/247,249.ccls. 340/$.ccls.) and ((certificate) same (password (pass adj (code word))) same user)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/04 17:14
13	5	(713/202.ccls. 709/224-229.ccls. 455.411.ccls. 380/247,249.ccls. 340/$.ccls.) and ((salt) same (password (pass adj (code word))))	USPAT; EPO; JPO; DERWENT; IBM_TDB	2003/12/04 17:14

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/519,829	03/06/2000	Sten-Olov Engberg	APRILS.001A	8563

20995 7590 12/15/2003

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER	
HENEGHAN, MATTHEW E	

ART UNIT	PAPER NUMBER
2134	10

DATE MAILED: 12/15/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

PRG

Office Action Summary	Application No.	Applicant(s)	
	09/519,829	ENGBERG ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 March 2000 and 12 March 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *28-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *28-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 March 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *4, 5, 6, 9*.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 28-53 have been examined. Claims 1-27 have been cancelled by preliminary amendment.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: item "712" in figure 7B. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: item "162" on page 7, lines 15 and 16 and page11, line 18; and item "702" on page 16, line 11. A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

4. The use of the trademarks Microsoft™, Windows NT™, UNIX™, Linux™, and NetWare™ has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 37-39 are rejected under 35 U.S.C. 102(b) as being anticipated by Australia Patent Application No. 63545/98 from Schmitz.

As per claims 37 and 39, Schmitz discloses a method in which the user of a device sends the qualifying identification (passcode) to an authorization computer, which generates a new TAN and sends it to the user in response to the request. The TAN created in the system disclosed by Schmitz functions as a temporary account that is activated upon the initial user request (see page 13, line 20 to page 14, line 10).

As per claim 38, the TAN may only be active for a predetermined amount of time (see page 18, lines 1-7).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 28-36 and 40-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Australia Patent Application No. 63545/98 from Schmitz in view of Menezes, "Handbook of Applied Cryptography," 1997, p. 390.

As per claims 28, 34, 35, 40, 41, and 43-53, Schmitz discloses a method in which the user of a device sends the qualifying identification (passcode) to an authorization computer, which generates a new TAN (token) and/or a password and sends them to the user in response to the request, who then transmits the password back to the authorization computer as part of a transaction or login (see page 13, line 20 to page 14, line 10).

Though Schmitz discloses that the authorization computer creates a password, no method for creating the password is taught.

Menezes discloses that a password may be augmented with a random string, called a "salt," along with a hashing function, in order to make dictionary attacks less effective (see section (v)), and further notes that an entity's ID can be used as a salt.

Therefore, 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 by 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.

As per claims 30, 31, 36, 42, Schmitz discloses that the user requests the token through the data input apparatus.

As per claims 32 and 33, Schmitz discloses that the device can be a pager or phone (see page 15, lines 24-29). Official notice is given that the reference to "handy" teaches to a mobile phone.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 5,153,919 to Reeds, III et al. discloses the creation of a password for a cell phone derived from a cell user's password and a salt.

U.S. Patent No. 5,497,411 to Pellerin discloses a procedure for user validation using a PIN.

U.S. Patent No. 5,875,394 to Daly et al. discloses a mutual authentication procedure for cell phones that uses two passwords together.

U.S. Patent No. 5,956,633 to Janhila discloses operator specific passwords created from multiple pieces of user information in a cell network.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (703) 305-7727. The examiner can normally be reached on Monday-Thursday from 8:00 AM - 4:00 PM Eastern Time. The examiner can also be reached on alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703) 872-9306
Hand-delivered responses should be brought to Crystal Park 2, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

MEH

December 4, 2003

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Notice of References Cited	Application/Control No. 09/519,829	Applicant(s)/Patent Under Reexamination ENGBERG ET AL.	
	Examiner Matthew Heneghan	Art Unit 2134	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-5,153,919	10-1992	Reeds et al.	380/44
	B	US-5,497,411	03-1996	Pellerin, Joseph C. E.	455/411
	C	US-5,875,394	02-1999	Daly et al.	455/411
	D	US-5,956,633	09-1999	Janhila, Pertti	455/410
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N	AU 9863545 A	11-1998	Australia	SCHMITZ, K	E05B 49/00
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Menezes, "Handbook of Applied Cryptography," 1997, p. 390
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

AU9863545

(12) PATENT ABSTRACT (11) Document No. AU-A-63545/98
(19) AUSTRALIAN PATENT OFFICE

(54) Title
METHOD FOR THE AUTHORIZATION IN DATA COMMUNICATION SYSTEMS

(51)[6] International Patent Classification(s)
H04L 009/32

(21) Application No. : **63545/98** (22) Application Date : **22/04/98**

(30) Priority Data

(31) Number	(32) Date	(33) Country
19718103	**29/04/97**	**DE GERMANY**

(43) Publication Date : **05/11/98**

(71) Applicant(s)
KIM SCHMITZ

(72) Inventor(s)
KIM SCHMITZ

(74) Attorney or Agent
GRIFFITH HACK , GPO Box 4164, SYDNEY NSW 2001

(57)

The invention relates to a method and to a device for the authorization in data transmission systems employing a transaction authorization number (TAN) or a comparable password. According to a first step, the user sends a qualifying identification of the data input apparatus together with a request for the generation or for the selection of a transaction authorization number TAN or of comparable password from a data file from the data input apparatus to an authorization computer. In a second step the authorization computer generates the transaction authorization number TAN or the comparable password or selects them form a data file. According to a third step, the authorization computer sends the transaction authorization number TAN or the comparable password over a second transmission path different from the first transmission path to a monitor, for example a handy or a pager. According to a fourth step, the user reads this transaction authorization number TAN or the comparable password from the receiver and enters the transaction authorization number TAN or the comparable password into the data input apparatus. According to a fifth step, this transaction authorization number TAN

.../2

or the comparable password is transmitted to the authorization computer. According to a sixth step, the authorization computer verifies the validity of the transaction-authorization number TAN or of the comparable password in order to establish or switch free, according to a seventh step, a connection between the data input apparatus and the receiver unit.

Regulation 3.2

AUSTRALIA

Patents Act 1990

ORIGINAL

COMPLETE SPECIFICATION

STANDARD PATENT

Invention Title: METHOD FOR THE AUTHORIZATION IN DATA COMMUNICATION SYSTEMS

The following statement is a full description of this invention, including the best method of performing it known to me:

GH REF: P25659-A:MHK:RK

METHOD POR AUTHORIZING IN DATA TRANSMISSION SYSTEMS

BACKGROUND OF THE INVENTION

1. Field of the Invention

The invention relates to a method for authorizing in data transmission and communication systems.

2. Brief Description of the Background of the Invention including Prior Art

It is known that in telebanking or in remote terminal banking the user requires in addition to his or her permanent password (personal identification number PIN) for each individual transaction additionally a transaction authorization number (TAN). Such transaction authorization numbers TANs are transmitted to the user in larger blocks by mail. Thus, there exists the risk that third persons receive knowledge of such transaction authorization numbers TANs and can perform a misuse in connection with the password. The risk is increased by such transaction authorization numbers TANs having a validity which is de facto unlimited in time.

Furthermore, call-back systems are known, wherein the called-in system assures based on a call-back at the generally stored telephone number that the calling system is authorized and that no foreign system pretends to be an authorized system. The disadvantage of the call-back systems comprises that an unauthorized user, who has procured a functional access to the authorized calling system from any possible source, can work without a problem based on this illegally obtained authorization, since the call-back system checks only whether the call-back system has been called by a system which is authorized in principle by a basically authorized system.

Summary of the Invention

At least preferred embodiments of the present invention furnish a method for authorizing and an authorization process in connection with data transmission and data communication, wherein the security of the transmission or communication is increased.

Brief Description of the Invention

In accordance with a first aspect of the present invention there is provided a method for the authorization of data transmission systems. A qualifying identification of a user is entered into a data input apparatus. The qualifying identification and a request for an authorization signal is transmitted from the data input apparatus to an authorization computer along a first transmission path. The authorization signal is established in the authorization computer. The authorization signal is sent from the authori-zation computer to a monitor along a second transmission path different as compared to the first transmission path. The authorization signal at the monitor is read by the user. The authorization signal is entered into the data input apparatus. The authorization signal is transmitted from the data input apparatus to the authorization computer. The validity of the authorization signal is verified in the authorization computer. A connection is established between the data input apparatus and a receiver unit upon verification of the validity of the authorization signal.

The authorization signal can be transmitted from the data input apparatus to the authorization computer along the first transmission path.

Acceptance of the authorization signal during verification of the validity of the authorization signal by the authorizing computer can be limited to a predefined number of times, to a predefined user time,

depending on a predetined number of data files being transmitted, or depending on a predefined size value of data files being transmitted.

A password can be employed for allowing accessing a member selected from the group consisting of the data input apparatus, the monitor, and the receiver unit.

The data transmitted from the data input apparatus to the receiver unit and vice versa or to the authorization computer and vice versa can be encoded.

An apparatus for authorizing access to a communication line includes a data input apparatus. An authorization computer is connected through a first transmission path to the data input apparatus. A monitor is connected to the authorization computer and disposed such that upon reading of an authorization signal on a monitor by a user, the user can enter the authorization signal into the data input apparatus. A receiver unit is connectable to the data input apparatus through a line switchable by the authorization computer between a connected state and a disconnected state.

The monitor can be a member selected from the group consisting of a pager, a handy, an email address, a net address, a telefax machine, a language output apparatus, an audio reproduction unit, a radio receiver, and a telephone.

The monitor can be a radio receiver incorporated into the data input apparatus. The radio receiver can furnish the authorization signal on a display monitor of the data input apparatus.

The radio receiver can include a user identification element furnished by a member selected from the group consisting of a magnetic card reader, a chip card reader, a graphic device for finger-print identification, and a graphic device for picture

identification.

A first encoding module can be present in the authorization computer. A second encoding module can be present in the monitor. The encoding provided by the first encoding module matches the encoding of the second encoding module.

The receiver unit can furnish a door-locking mechanism.

The authorization computer and the receiver unit can be integrated into a single apparatus. Furthermore, the data input apparatus, the authorization computer, and the receiver unit can be integrated into one single apparatus.

Wireless telecommunication apparatuses, such as for example Handys (Handie-Talkie is a tradename of the Motorola Communications Division) or pagers, are frequently furnished with the possibility to receive short alphanumeric communications, for example of the Short Message Service known in Germany as SMS-DIENST, and to display these communications on their display screen. A paging system is a communications system for summoning individuals such as doctors and nurses or for making public announcements. The present invention employs this possibility to receive short alphanumeric communications in order to transmit a transaction authorization number or a comparable password.

In accordance with the first aspect of the present invention. the user transmits his or her identification, such as user identification, password, or the like, and/or an identification characterization of the data input apparatus together with a request for generating a transaction authorization number TAN, or a comparable password, to a computer through a data input apparatus. The computer furnishes the authorization process and is therefore called in the following by the abbreviation

authorizing computer. An alphanumeric or only numeric transaction authorization number TAN, or a comparable password, is calculated or read from a data file based on a random number generator in this authorization computer. This transaction authorization number TAN, or a similar password, is transmitted to a receiver by the authorizing computer through another transmission path disposed parallel to the existing connection with the data-input apparatus. This receiver can be for example:

a) a wireless receiver with a display or a monitor such as for example a handy, a pager (for example a city-call receiver),

b) a specially constructed receiver card within the data input apparatus, which is accessed wirelessly or through a fixed wiring;

c) a mailbox;

d) a telefax apparatus; or

e) a language output apparatus such as a fixed installed audio speaker or a telephone for the language transmission.

The authorization computer includes a memory storage and has available the required telephone numbers, wireless call numbers, or fax numbers, email addresses or network addresses. The data reterring to this are usually stored in the authorization computer. However, it is possible that the authorization computer in turn shares and/or retrieves these data from a data source, which data source is resident on another computer. In addition, the authorization computer can also access this other computer on its own by using the method according to the present invention.

The authorized user can enter the thus transmitted transaction authorization number or the comparable password manually into his/her data input apparatus and send the transaction authorization number TAN again to

the authorization computer. An automatic transmission of the transaction authorization number TAN or of the comparable password occurs according to the present invention in case of an automatic procedure. The authorization computer checks and verifies now the congruence and agreement between all valid transaction authorization numbers TANs or comparable passwords previously given out by the authorizing computer, and the authorization computer allows a release of the data flow between the data input apparatus and a receiver unit after this checking of the authorization.

The transaction authorization number or the comparable password can be a transaction authorization number for one single use. However, other limitations such as the user time and/or the number or the size of the data files to be transmitted relating are also conceivable for use in determining the validity of the transaction authorization number or of the comparable password.

Now, data can be transmitted from the data input apparatua to the receiver unit and vice versa, for example by full duplex, after a connection authorized in the above described manner has been established.

It is clear that these data can also be encrypted or encoded first and then transmitted for obtaining additional security.

Both the data input apparatus, as well as the authorization computer and the receiver unit can be furnished as standard personal computers. The present invention operates independent from the platform employed, i.e. independent of the type of processor, of the operating system and/or of the control electronics, for example of the receiver unit, and/or of the input/output units, for example of the data input apparatus and of the receiver unit.

The security of this system is based on the fact that a data transmission from the data input apparatus to the receiver unit has to be released and turned on by the authorization computer only in case of an authorization of the apparatus. This is accomplished by the employment of separate transmission paths between the data input apparatus and the authorization computer on the one hand, and between the authorization computer and the transaction-authorization-number transmission on the other hand. The present invention is insofar distinguished from call-back systems, where only one checking occurs between the data input apparatus and the authorization computer.

The method according to a first aspect of the present invention allows to provide a number of different levels of security.

A wireless receiver, for example in the form of a plug-in card, is incorporated as a receiver in the data input apparatus, representing the lowest security level such that a data transmission is possible to the receiver unit only with this concrete apparatus. In order to increase this security, it can be provided that this wireless receiver can only be operated with a user identification element, for example a magnetic card or a chip card. The user identification element can also operate with graphical methods, such as testing, verification and/or identification of a fingerprint or of a picture identification of the user.

The further security level provides that the authorization computer transmits the transaction authorization number or the comparable password to a pager or a comparable apparatus. In this case, an authorization is furnished only when the data input apparatus and the pager are accessed by the same person. Only then is it possible that the transaction authorization number or a

comparable password, displayed on the pager, are entered into the data input apparatus and are transmitted from there again to the authorization computer.

Data transmitted to a pager can however be branched off and be listened to. A further security step can be obtained in the manner that matching encoding or encryption modules are employed in the authorization computer and in the pager.

Another receiver apparatus can be furnished instead of the pager or the handy. This can for example be a mailbox, a telefax, a language output apparatus, a sound-receiver printed circuit board or an audio-response unit. Fixedly installed audio speakers or the transmission of the audio or voicemail to a defined telephone connection are possible to serve as an audio output unit and audio-response unit. An audio output of the transaction authorization number or of the comparable password is performed with the language output apparatus or audio-response unit.

The transmission to such receiver apparatuses can also be encoded and/or encrypted.

Further encoding mechanisms can be dispensed with if one employs a handy, in particular a GSM handy, instead of a pager based on the encoding of the respective transmission technique. In this case, the display of the transaction authorization number or of the comparable password is performed on the display of the handy.

A further step of security can be accomplished by establishing a connection between the data input apparatus and the authorization computer only when a corresponding password is transmitted through the data input apparatus. This password can be valid according to the present invention for a time, which is substantially longer than the transfer authorization number TAN.

A further step of security can be achieved by, requiring also a password already for the use of the data

input apparatus.

It is apparent that a combination of the precedingly recited step of security is possible.

In accordance with a second aspect of the present invention there is provided an apparatus for authorizing access to a communication line comprising a data input apparatus, an authorization computer connected through a first transmission path to the data input apparatus, a monitor connected to the authorization computer and disposed such that upon reading of an authorization signal on a monitor by a user, the user can enter the authorization signal into the data input apparatus; a receiver unit connectable to the data input apparatus through a line switchable by the authorization computer between the connected state and a disconnected state.

The present invention can be universally employed in the region of data transmission systems. This holds for example also for the Internet and intranets, local area networks LAN, wide area networks WAN, etc.

The system in question can also be employed outside of the classic electronic data processing, for example in connection with physical access controls. For this purpose, the user enters for example his or her personal password on a keyboard, representing a data input apparatus, and located next to a door. The authorization computer checks and verifies this password, possibly also in connection with the access permission to the concrete space at the concrete time. If the respective password is still valid, then the authorization computer provides the transaction authorization number or the comparable password to a handy or to an apparatus conceived for the special door closing system and functionally comparable with the pager. In the following, this transaction authorization number or the comparable password is

entered manually by the user to a keyboard disposed in proximity of the door and is further transmitted automatically to the authorization computer. After a successful verification, a signal is provided by the authorization computer for a release of the door-locking mechanism. The release can be limited in time, if desired. The receiver unit can in this case be of the most simple nature relative to its technological construction, since the receiver unit only has to process the signal for the release of the door-locking mechanism in such a way that the respective electro-mechanical system releases the door for opening.

Thus, it is possible to construct a system where different persons have different authorizations for accessing different rooms.

The concrete fields of application comprise, for example:

computer centers
airports
ministries, government offices
customs
border transition points
security regions
banks
police and military applications
shielded storage, vaults, bank vaults
garages
parking houses
automobiles

The complete system receives its security from the combination of several different base principles and factors:

(1) "what you have" (the GSM chip card riot to be duplicated), i.e. a physically unique structure which

cannot be transferred without loss.

(2) "what you know" (the PIN of the GSM chip card as well as the own user names in the data input apparatus and/or the authentication server), i.e. know-how which cannot be transferred without intent or by mistake.

(3) DES-encoding and cryptographic authentication in the GSM net itselfi whereby resistance against listening attacks and manipulating attacks is obtained.

The combination of at least three events, which events by themselves are already very improbable, is necessary for a compromising of the system;

a) physical loss of the handy chip card, of the pager, or a foreign access to the mailbox, to the telefax, to the language output apparatus, or to the audio-delivery unit,

b) giving out of the PIN number of the receiver (for example of the chip card or of the handy) and

c) knowledge of the transmitted transaction authorization number or of the comparable password.

An inadvertent coincidence of these factors is nearly excludable, since also in this case the successful attack on the system presupposes the intimate knowledge of the access procedure and of the user identification ID, which is usually not present in case of an attack. In addition, the user has the possibility to block immediately or to have blocked immediately his or her user identification ID at the authentication server upon a loss of his or her chip card.

A further advantage of the support of the GSM can be that the user is reachable all the time during the authorization process, i.e. the user can be directly called by the system administrator in case of access problems or doubts in regard to the identity of the user.

This solution is associated with the advantage that

the solution is very secure, low cost, and realizable with widely available and secure, conventional hardware.

A further solution according to the present invention comprises that the authorization computer and the receiver unit are present as a single apparatus.

The present invention may be more fully understood from the description of preferred embodiments given below with reference to the accompanying drawings, by way of example only.

Brief Description of the Drawings

In the accompanying drawing, in which are shown several of the various possible embodiments of the present invention:

Fig. 1 is a view of a schematic diagram showing an operational system employing authorization in data transmission.

Description of Invention and Preferred Embodiment

The user sends according to a first step his or her qualifying identification through a data input apparatus 1, together with a request for generating or for selecting a transaction authorization number TAN or a comparable password from a data file, to an authorization computer 2. The authorization computer 2 generates the transaction authorization number TAN or the comparable password or selects the transaction authorization number TAN or the comparable password from a data file according to a second step. The authorization computer 2 sends the transaction authorization number TAN or the comparable password through a different transmission path as compared to the transmission path of the first step to a receiver 3 according to a third step. The user takes this transaction authorization number TAN or the comparable password from the receiver 3 and enters the transaction authorization

number TAN or the comparable password into the data input apparatus 1 according to a fourth step. This transaction authorization number TAN or the comparable password is transmitted again to the authorization computer 2 according to a fifth step. The authorization computer 2 verifies the validity of the transaction authorization number TAN or of the comparable password according to a sixth step, in order to establish a connection between the data input apparatus 1 and a receiver unit 4 according to a seventh step.

The transaction authorization number TAN or the comparable password can be a one-time usable transaction authorization number TAN or a one time usable password. The validity of the transaction authorization number TAN or of the comparable password can be limited to a predefined user time. The validity of the transaction authorization number TAN or of the comparable password can be dependent on a predefined number of the transmitted data files or on a predefined size value of the transmitted data files.

Access to the data input apparatus 1 and/or to the receiver 3 and/or the receiver unit 4 can be protected by a password. The data transmitted from the data input apparatus 1 to the receiver unit 4 or vice versa can be encoded and the data transmitted from the data input apparatus 1 to the authorization computer 2 or vice versa are encoded.

The apparatus for the authorization of data transmission systems includes a data input apparatus 1 serving for entering a qualifying identification of a user into the data input apparatus 1 and for transmitting the qualifying identification and a request for an authorization signal from the data input apparatus 1 to the authorization computer 2 along a first transmission path. The authorization computer 2

serves for establishing the authorization signal in the authorization computer 2, and for sending the authorization signal from the authorization computer 2 to a monitor 3 along a second transmission path different as compared to the first transmission path. The monitor 3 serves for reading the authorization signal at the monitor 3 by the user. The data input apparatus 1 further serves for entering the authorization signal into the data input apparatus 1 by the user and for transmitting the authorization signal from the data input apparatus 1 to the authorization computer 2. The authorization computer 2 further serves for verifying the validity of the authorization signal in the authorization computer 2 and for establishing a connection between the data input apparatus 1 and the receiver unit 3 upon veriticatIon of the validity of the authorization signal.

The receiver 3 can be a pager 31 or a handy 32. The receiver 3 can also be an email address or a net address, a telefax machine 33, or a language output apparatus or an audio reproduction unit. The language output apparatus or the audio reproduction unit can be a loud and audio speaker 34 or a telephone 35.

The receiver 3 can be a radio receiver incorporated into the data input apparatus 1. The radio receiver can furnish the transaction authorization number TAN or the comparable password on the display or monitor of the data input apparatus 1. The radio receiver can include a user identification element.

The user identification element can be a magnetic card or a chip card. The user identification element can operate with graphic devices for verifying a finger print or for a picture identification of the user.

Matching encoding modules can be present in the authorization computer 2 and in the receiver 3.

The receiver element 4 can be a door-locking mechanism.

The authorization computer 2 and the receiver unit 4 can be integrated into a s]Lngle apparatus. The data input apparatus, the authorization computer 2, and the receiver unit 4 can be integrated into one single apparatus.

An authorized user actuates a data input apparatus 1. The authorized user enters and sends 101 a request tor generating or for selecting and returning a transaction authorization number TAN or a comparable password to an authorization computer 2 along a transmission path 102 from the data input apparatus 1 to the authorization computer 2. The authorization computer 2 generates a transaction signal such as the transaction authorization number TAN or a comparable password. The authorization computer 2 can derive the authorization signal from a random number generator 5 or from a data file contained in the authorization computer 2. The authorization computer 2 knows the telephone number or the data address, for example the email address or net address of the receiver 3 of the user of the data input apparatus 1. The authorization computer 2 sends this transaction authorization number TAN or a comparable password to a monitor representing the receiver 3 along a transmission path 103 from the authorization computer 2 to the monitor or receiver 3. The receiver 3 can be a pager 31 or a handy 32. The receiver 3 however can also be provided as the email address of a mailbox 37 and displayed on a monitor 36, a telefax apparatus 33, or a language output apparatus or audioreproduction unit. The audio-reproduction unit can be a fixedly installed audio speaker 34 or a telephone 35. The language output apparatus can be a computer 38 reconstituting language into sound or text

files.

The monitor can be a radio receiver incorporated into the data input apparatus, wherein the radio receiver furnishes the authorization signal on a display monitor of the data input apparatus. The radio receiver can include a user identification element furnished by an access card such as a magnetic card or a chip card.

The user reads this transaction authorization number or a comparable password from the receiver 3 or hears the transaction authorization number TAN from the language or audio output and enters 104 it manually into the data input apparatus 1. The data input apparatus 1 now transmits the transaction authorization number TAN or the comparable password to the authorization computer 2 along a transmission path 105 from the data input apparatus 1 to the authorization computer 2. The authorization computer 2 verifies if this transaction authorization number TAN or the comparable password are still valid. For this purpose, the authorization computer can be programmed such that the validity of the transaction authorization number or of the comparable password is limited in time between its emission to the receiver 3 and its transmission through the data input apparatus 1. The time period limitation can for example amount to two minutes. If the transaction authorization number TAN or the comparable password are valid, then the authorization computer 2 furnishes a connection 107, 108 from the data input apparatus 1 to the receiver unit 4. Now the user is able to transmit and/or to receive data from the data input apparatus 1 to the receiver unit 4 for the time period this connection 107, 108 is maintained.

It is apparent that these data can be encrypted and encoded for additional security.

It is further conceivable that not only the transaction authorization number TAN or the comparable password have a time limitation with respect to their validity, but that also the time duration of the maintaining of the connection 107, 108 between the data input apparatus 1 and the receiver apparatus 4 is limited in time. Thereby, it can be avoided that a "standing" line is furnished between the data input apparatus 1 and the receiver unit 4, which gain could represent a hole in the security system.

The authorization computer 2 and the receiver uni-t 4 can be furnished by a single computer. In this case, a first access is performed to a data processing program, which performs the authorization process, including generation and transmission of the transaction authorization number TAN, in the manner precedingly described. The data transmission is then performed as a second step.

The data input apparatus 1, the authorization computer 2 and the receiver unit 4 can even be a single computer. in this case, a first access is performed to a data processing program, which performs the authorization process, including generation and transmission of the transaction authorization number TAN, to the receiver in the way described above. The user obtains full access to or access limited to specific regions of the computer only after authorization.

It will be understood that each of the elements described above, or two or more together, may also find a useful application in other types of authorization processes differing from the types described above.

While the invention has been illustrated and described as embodied in the context of a method for the authorization in data transmission systems, it is

not intended to be limited to the details shown, since various modifications and structural changes may be made without departing in any way from the spirit of the present invention.

Without further analysis, the foregoing will so fully reveal the gist of the present invention that others can, by applying current knowledge, readily adapt it for various applications without omitting features that, from the standpoint of prior art, fairly constitute essential characteristics of the generic or specific aspects of this invention.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A method for the authorization of data transmission systems comprising

entering a qualifying identification of a user into a data input apparatus;

transmitting the qualifying identification and a request for an authorization signal from the data input apparatus to an authorization computer along a first transmission path;

establishing the authorization signal in the authorization computer;

sending the authorization signal from the authorization computer to a monitor along a second transmission path different as compared to the first transmission path;

reading the authorization signal at the monitor by the user;

entering the authorization signal into the data input apparatus;

transmitting the authorization signal from the data input apparatus to the authorization computer.
verifying the validity of the authorization signal in the authorization computer;

establishing a connection between the data input apparatus and a receiver unit upon verification of the validity of the authorization signal.

2. The method according to claim 1 wherein the authorization signal is transmitted from the data input apparatus to the authorization computer along the first transmission path.

3. The method according to claim 1 or 2; further comprising limiting acceptance of the authorization signal during verification of the validity of the authorization signal by the authorizing computer to a predefined number of times.

4. The method according to any one of the preceding claims, further comprising limiting acceptance of the authorization signal during verification of the validity of the authorization signal by the authorizing computer to a predefined user time.

5. The method according to any one of the preceding claims, further comprising limiting acceptance of the authorization signal during verification of the validity of the authorization signal by the authorizing computer depending on a predefined number of data files being transmitted.

6. The method according to any one of the preceding claims, further comprising limiting acceptance of the authorization signal during verification of the validity of the authorization signal by the authorizing computer depending on a predefined size value of data files being transmitted.

7. The method according to any one of the preceding claims further comprising employing a password for allowing accessing a member selected from the group consisting of the data input apparatus, the monitor, and the receiver unit.

8. The method according to any one of the preceding claims, further comprising encoding the data transmitted from the data input apparatus to the receiver unit and vice versa.

9. The method according to any one of the preceding claims, further comprising encoding the data transmitted from the data input apparatus to the authorization computer and vice versa.

10. A method for the authorization of data transmission systems employing a transaction authorization number (TAN) or a comparable password,
wherein a user sends according to a first step his or her qualifying identification through a data input apparatus,

together with a request for generating or for selecting a transaction authorization number TAN or a comparable password from a data file, to an authorization computer, wherein the authorization computer generates the transaction authorization number TAN or the comparable password or selects the transaction authorization number TAN or the comparable password from a data file according to a second step, wherein the authorization computer sends the transaction authorization number TAN or the comparable password through a different transmission path as compared to the transmission path of the first step to a receiver according to a third step, wherein the user takes this transaction authorization number TAN or the comparable password from the receiver and enters the transaction authorization number TAN or the comparable password into the data input apparatus according to a fourth step, wherein thistransaction authorization number TAN or the comparable password is transmitted again to the authorization computer according to a fifth step, wherein the authorization computer verifies the validity of the transaction authorization number TAN or of the comparable password according to a sixth step, in order to establish a connection between the data input apparatus and a receiver unit according to a seventh step.

11. The method according to claim 10, wherein the transaction authorization number TAN or the comparable password is a one-time usable transaction authorization number TAN or a one time usable password; wherein the validity of the transaction authorization number TAN or of the comparable password is limited to a predefined user time; wherein the validity of the transaction authorization number TAN or of the comparable password is dependent on a predefined number of the transmitted data files; wherein the validity of the transaction authorization number TAN or of the comparable password is dependent on a predefined

size value of the transmitted data files.

12. The method according to claim 10, wherein access to the data input apparatus and/or to the receiver and/or the receiver unit is protected by a password; wherein the data transmitted from the data input apparatus to the receiver unit or vice versa are encoded; wherein the data transmitted from the data input apparatus to the authorization computer or vice versa are encoded.

13. An apparatus for authorizing access to a communication line comprising a data input apparatus; an authorization computer connected through a first transmission path to the data input apparatus; a monitor connected to the authorization computer and disposed such that upon reading of an authorization signal on a monitor by a user, the user can enter the authorization signal into the data input apparatus; a receiver unit connectable to the data input apparatus through a line switchable by the authorization computer between a connected state and a disconnected state.

14. The apparatus according to claim 13, wherein the monitor is a member selected from the group consisting of a pager, a handy, an email address, a net address, a telefax machine, a language output apparatus, an audio reproduction unit, a radio receiver, and a telephone.

15. The apparatus according to claim 13 or 14, wherein the monitor is a radio receiver incorporated into the data input apparatus, wherein the radio receiver furnishes the authorization signal on a display monitor of the data input apparatus.

16. The apparatus according to any one of claims 13-15 wherein the radio receiver includes a user identification element furnished by a member selected from the group consisting of a magnetic card reader, a chip card reader, a graphic device for finger-print identification, and a graphic device for picture identification.

17. The apparatus according to any one of claims 13-16 comprising a first encoding module present in the authorization computer; a second encoding module present in the monitor, wherein an encoding provided by the first encoding module matches an encoding of the second encoding module.

18. The apparatus according to any one of claims 13-17, wherein the receiver unit furnishes a door-locking mechanism.

19. The apparatus according to any one of claims 13-18, wherein the authorization computer and the receiver unit are integrated into a single apparatus.

20. The apparatus according to any one of claims 13-19, wherein the data input apparatus, the authorization computer, and the receiver unit are integrated into one single apparatus.

21. The apparatus according to any one of claims 13-20, wherein the data input apparatus serves for entering a qualifying identification of a user into the data input apparatus and for transmitting the qualifying identification and a request for an authorization signal from the data input apparatus to the authorization computer along a first transmission path; wherein the authorization computer serves for establishing the authorization signal in the authorization computer, and for sending the authorization signal from the authorization computer to a monitor along a second transmission path different as compared to the first transmission path; wherein the monitor serves for reading the authorization signal at the monitor by the user; wherein the data input apparatus further serves for entering the authorization signal into the data input apparatus by the user and for transmitting the authorization signal from the data input apparatus to the authorization computer; wherein the authorization computer further serves for verifying the validity of the

authorization signal in the authorization computer and for establishing a connection between the data input apparatus and the receiver unit upon verification of the validity of the authorization signal.

22. A method for authorization of data transmission systems substantially as herein described with reference to the accompanying drawing.

23. An apparatus for authorizing access to a communication line substantially as herein described with reference to the accompanying drawing.

Dated this 22nd day of April 1998

KIM SCHMITZ

By his Patent Attorney

GRIFFITH HACK

ABSTRACT OF THE DISCLOSURE

The invention relates to a method and to a device for the authorization in data transmission systems employing a transaction authorization number (TAN) or a comparable password. According to a first step, the user sends a qualifying identification of the data input apparatus together with a request for the generation or for the selection of a transaction authorization number TAN or of comparable password from a data file from the data input apparatus to an authorization computer. In a second step the authorization computer generates the transaction authorization number TAN or the comparable password or selects them form a data file. According to a third step, the authorization computer sends the transaction authorization number TAN or the comparable password over a second transmission path different from the first transmission path to a monitor, for example a handy or a pager. According to a fourth step, the user reads this transaction authorization number TAN or the comparable password from the receiver and enters the transaction authorization number TAN or the comparable password into the data input apparatus. According to a fifth step, this transaction authorization number TAN or the comparable password is transmitted to the authorization computer. According to a sixth step, the authorization computer verifies the validity of the transaction-authorization number TAN or of the comparable password in order to establish or switch free, according to a seventh step, a connection between the data input apparatus and the receiver unit.

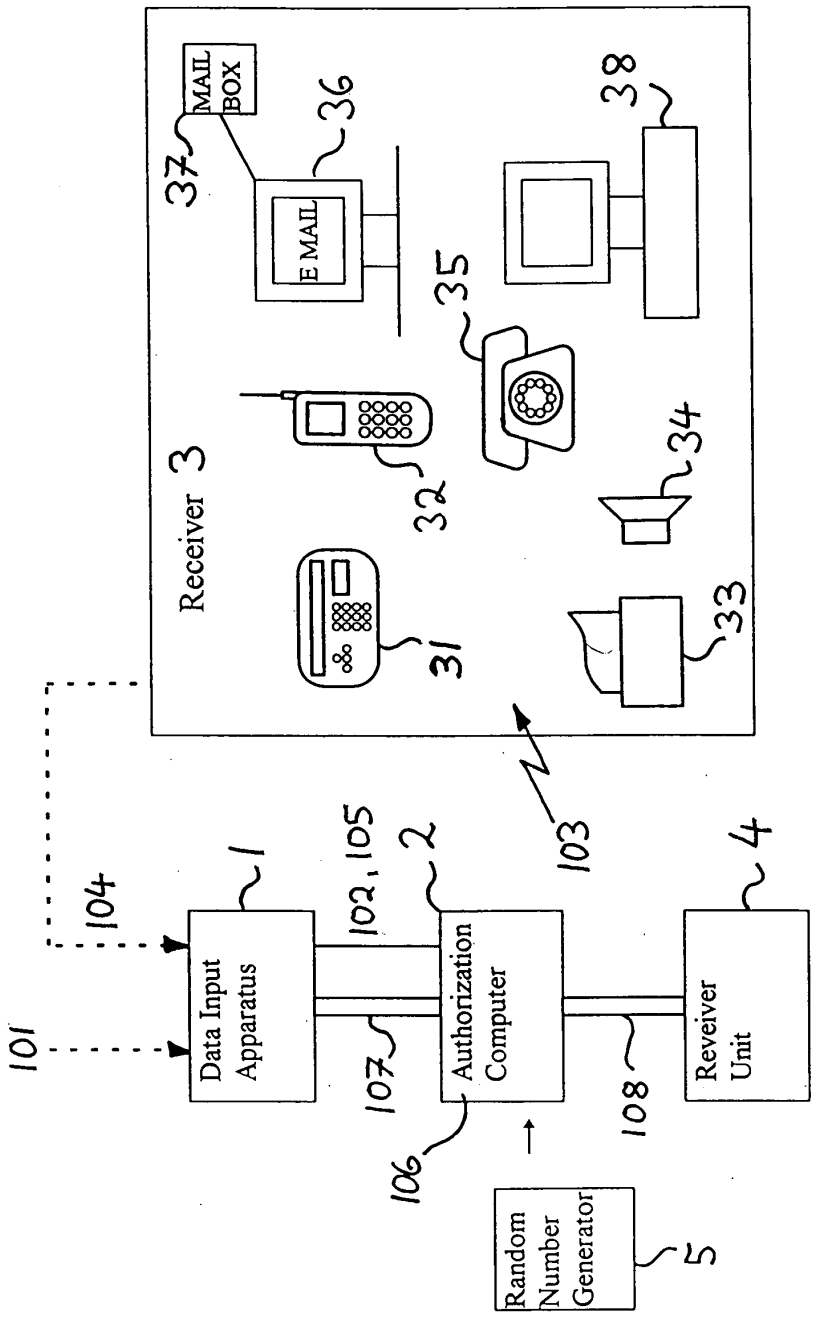

Receiver 3
MAIL BOX
37
E MAIL
36
38
35
34
32
31
33
101
104
Data Input Apparatus
1
102, 105
2
Authorization Computer
103
4
Reveiver Unit
107
106
108
Random Number Generator
5

Fig. 1

BEST AVAILABLE COPY

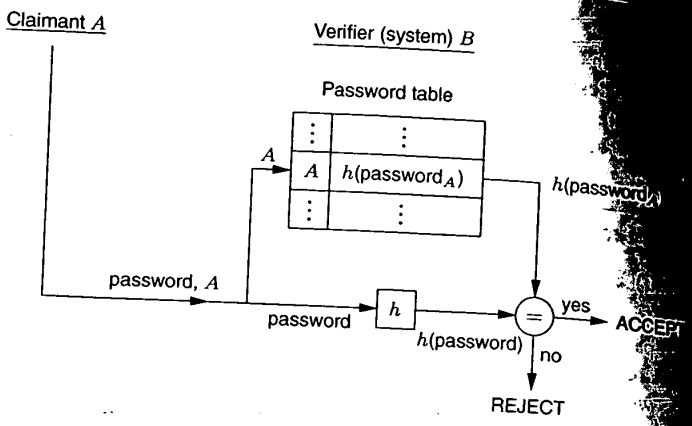


Figure 10.1: *Use of one-way function for password-checking.*

Another procedural technique intended to improve password security is *password aging*. A time period is defined limiting the lifetime of each particular password (e.g., 30 or 90 days). This requires that passwords be changed periodically.

(iv) Slowing down the password mapping

To slow down attacks which involve testing a large number of trial passwords (see §10.2.2), the password verification function (e.g., one-way function) may be made more computationally intensive, for example, by iterating a simpler function $t > 1$ times, with the output of iteration i used as the input for iteration $i + 1$. The total number of iterations must be restricted so as not to impose a noticeable or unreasonable delay for legitimate users. Also, the iterated function should be such that the iterated mapping does not result in a final range space whose entropy is significantly decimated.

(v) Salting passwords

To make dictionary attacks less effective, each password, upon initial entry, may be augmented with a t-bit random string called a *salt* (it alters the "flavor" of the password; cf. §10.2.3) before applying the one-way function. Both the hashed password and the salt are recorded in the password file. When the user subsequently enters a password, the system looks up the salt, and applies the one-way function to the entered password, as altered or augmented by the salt. The difficulty of exhaustive search on any particular user's password is unchanged by salting (since the salt is given in cleartext in the password file); however, salting increases the complexity of a dictionary attack against a large set of passwords simultaneously, by requiring the dictionary to contain 2^t variations of each trial password, implying a larger memory requirement for storing an encrypted dictionary, and correspondingly more time for its preparation. Note that with salting, two users who choose the same password have different entries in the system password file. In some systems, it may be appropriate to use an entity's userid itself as salt.

(vi) Passphrases

To allow greater entropy without stepping beyond the memory capacity of human users, passwords may be extended to *passphrases*; in this case, the user types in a phrase or sentence rather than a short "word". The passphrase is hashed down to a fixed-size value, which plays the same role as a password; here, it is important that the passphrase is not simply trun-

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. APRILS.001A	APPLICATION NO. 09/519,829
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (USE SEVERAL SHEETS IF NECESSARY)	APPLICANTS Engberg, et al.	
	FILING DATE March 6, 2000	GROUP ART UNIT 2777

OIPE MAY 23 2000 PATENT & TRADEMARK OFFICE

RECEIVED MAY 25 2000 TECH CENTER 2700

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPROPRIATE)

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO

EXAMINER INITIAL		OTHER DOCUMENTS (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
MH 12/3/03		24-hour cellphone cyberwatch - Internet - printed on 5/19/00.
MH 12/3/03		Monkey as authentication software - Internet - 2 pages, printed on 5/19/00.
MH 12/3/03		Monkey (mobile network key) - Internet - 6 pages, printed on 5/19/00.

H:\DOCS\ASF\ASF-1435.DOC\dns
051900

EXAMINER M. Hall	DATE CONSIDERED 12/3/03

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. APRILS.001A	APPLICATION NO. 09/519,829
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (USE SEVERAL SHEETS IF NECESSARY)	APPLICANTS Engberg, et al.	
	FILING DATE March 6, 2000	GROUP ART UNIT 2777

OIPE JC03 AUG 0 8 2000 PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPROPRIATE)

RECEIVED AUG 11 2000 TC 2700 MAIL ROOM

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO
MH 12/3/03		AU-A-63545/98	05/11/98	Australia				
MH 12/3/03		EP 0 875 871 A2	11/04/98	European — see US Patent 6,078,908 MH				

EXAMINER INITIAL		OTHER DOCUMENTS (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)

H:\DOCS\ASF\ASF-1531.DOC\dns
080200

EXAMINER MH	DATE CONSIDERED 12/3/03

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. APRILS.001A	APPLICATION NO. 09/519,829
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	APPLICANTS Engberg, et al.	
(USE SEVERAL SHEETS IF NECESSARY)	FILING DATE March 6, 2000	GROUP ART UNIT 2777

RECEIVED
JAN 18 2001
Technology Center 2100
OIPE JC8 JAN 12 2001 PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPROPRIATE)
MH 12/3/03		6,078,908	06/20/00	Schmitz	705	50	April 22, 1998

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO

EXAMINER INITIAL		**OTHER DOCUMENTS** (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)

H:\DOCS\ASF\ASF-1800.DOC\dns\010801

EXAMINER MH	DATE CONSIDERED 12/3/03

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

#9

SHEET 1 OF 1

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY. DOCKET NO. APRILS.001A	APPLICATION NO. 09/519,829
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (USE SEVERAL SHEETS IF NECESSARY)	APPLICANTS Engberg, et al.	
	FILING DATE March 6, 2000	GROUP ART UNIT 2777

PATENT & TRADEMARK OFFICE AUG 09 2001 OIPE

RECEIVED AUG 13 2001 Technology Center 2100

U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPROPRIATE)
MH 12/3/03		5,590,198	12/31/96	Lee, et al.			
MH 12/3/03		5,923,763	07/13/99	Walker, et al.			
MH 12/3/03		6,049,877	04/11/00	White			
MH 12/3/03		6,161,182	12/12/00	Nadooshan			
MH 12/3/03		US 6,173,400 B1	01/09/01	Perlman, et al.			

FOREIGN PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION	
							YES	NO

EXAMINER INITIAL		OTHER DOCUMENTS (INCLUDING AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.)
MH 12/3/03		International Search Report for PCT/US01/07058 (3-pages).

H:\DOCS\ASF\ASF-2342.DOC\dns\080301

EXAMINER M. H.	DATE CONSIDERED 12/3/03

*EXAMINER: INITIAL IF CITATION CONSIDERED, WHETHER OR NOT CITATION IS IN CONFORMANCE WITH MPEP 609; DRAW LINE THROUGH CITATION IF NOT IN CONFORMANCE AND NOT CONSIDERED, INCLUDE COPY OF THIS FORM WITH NEXT COMMUNICATION TO APPLICANT.

Docket No.: APRILS.001A

03-12-04

2134

Customer No.: 20,995

OIPE
MAR 1 1 2004
JC35
PATENT & TRADEMARK OFFICE

AMENDMENT / RESPONSE TRANSMITTAL

Applicant	:	Sten-Olov Engberg et al.
App. No.	:	09/519,829
Filed	:	March 6, 2000
For	:	USE OF PERSONAL Communication DEVICES FOR USER AUTHENTICATION
Examiner	:	Matthew E. Heneghan
Art Unit	:	2134
Confirmation No.	:	8563

Certificate of Express Mail
Under 37 C.F.R. § 1.10

Express Mail No.
EV 307 986 855 US

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as "Express Mail Post Office to Addressee" in an envelope addressed to:

United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450

on

March 11, 2004
(Date)

Jerry T. Sewell, Reg. No. 31,567

RECEIVED
MAR 1 5 2004
Technology Center 2100

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

Transmitted herewith for filing in the above-identified application are the following enclosures:

(X) Amendment and Response to December 15, 2003 Office Action in 14 pages.

(X) Two sheets of replacement drawings.

(X) The present application qualifies for small entity status under 37 C.F.R. § 1.27.

The fee has been calculated as shown below:

FEE CALCULATION				
FEE TYPE		**FEE CODE**	**CALCULATION**	**TOTAL**
Total Claims	26 - 26 = 0	2202 ($9)	0 x 9 =	$0
Independent Claims	5 - 5 = 0	2201 ($43)	0 x 43 =	$0
			TOTAL FEE DUE	**$0**

(X) Return prepaid postcard.

(X) Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Jerry T. Sewell
Registration No. 31,567
Attorney of Record
Customer No. 20,995
(949) 760-0404

JTS-19400.DOC // 20040311/2

OIPE JC35
MAR 1 1 2004
PATENT & TRADEMARK OFFICE

#11/B

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Sten-Olov Engberg et al.
Appl. No.	:	09/519,829
Filed	:	March 6, 2000
For	:	USE OF PERSONAL Communication DEVICES FOR USER AUTHENTICATION
T.C./A.U.	:	2134
Examiner	:	Matthew E. Heneghan
Atty Docket No.	:	APRILS.001A
Confirmation No.	:	8563
Customer No.	:	20,995

RECEIVED
MAR 1 5 2004
Technology Center 2100

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450

AMENDMENT AND RESPONSE TO DECEMBER 15, 2003 OFFICE ACTION

Dear Sir:

In response to the December 15, 2003 Office Action, Applicants respectfully submit the following amendments and remarks.

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Amendments to the Drawings begin on page 7 of this paper and include an attached *Replacement Sheet* for each sheet of drawings being amended.

Remarks/Arguments begin on page 8 of this paper.

Appl. No.	**:**	**09/519,829**
Filed	**:**	**March 6, 2000**
Office Action Date	**:**	**December 15, 2003**

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application. The listing of claims present each claim with its respective status shown in parentheses.

In the following list, Claim 37 is currently amended. Claims 28-36 and 38-53 remain as previously presented.

Listing of Claims

Claims 1 - 27 Cancelled.

Claim 28 (Previously presented): 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.

B1

Claim 29 (Previously presented): The method of Claim 28, wherein the new password is generated by concatenating the token and the passcode.

Claim 30 (Previously presented): The method of Claim 28, further comprising receiving a request from the user for the token.

Claim 31 (Previously presented): The method of Claim 30, wherein the request is transmitted by the user through the personal communication device.

Claim 32 (Previously presented): The method of Claim 28, wherein the personal communication device is a mobile phone.

Claim 33 (Previously presented): The method of Claim 28, wherein the personal communication device is a pager.

Claim 34 (Previously presented): A user authentication system comprising:

a user database configured to associate a user with a personal communication device possessed by the user;

a control module 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;

a communication module configured to transmit the token to the personal communication device; and

an authentication module configured to receive the password from the user.

Claim 35 (Previously presented): The system of Claim 34, 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.

B1

Claim 36 (Previously presented): The system of Claim 35, wherein the request is transmitted by the user through the personal communication device.

Claim 37 (Currently Amended): A method of regulating access to a secure system, the method comprising:

associating [[the]] a user with a personal communication device possessed by the user;

associating the user with an account, wherein an initiation of access through the account requires that the account be activated;

receiving a request transmitted by the personal communication device; and

in response to the receipt of the request, activating the account.

Claim 38 (Previously presented): The method of Claim 37, further comprising deactivating the account within a predetermined amount of time after the account is activated.

Claim 39 (Previously presented): The method of Claim 37, wherein an initiation of access through the account further requires that the user supply a valid password.

Claim 40 (Previously presented): The method of Claim 39, further comprising:

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 the valid password to be the new password;

transmitting the token to the personal communication device; and

receiving the valid password from the user.

Claim 41 (Previously presented): The method of Claim 40, wherein the new password is generated by concatenating the token and the passcode.

B1

Claim 42 (Previously presented): The method of Claim 40, wherein the token is transmitted in response to the receipt of the request.

Claim 43 (Previously presented): A method of regulating access to a secure system, the method comprising:

receiving a request for a token, wherein the request is transmitted from a personal communication device as a result of an action by a user;

in response to the receipt of the request, transmitting the token to the personal communication device;

receiving login data from the user in response to a request for authentication information, wherein the login data is based at least upon the token; and

granting access to the secure system based at least upon the received login data.

Claim 44 (Previously presented): The method of Claim 43, wherein the login data is additionally based upon a passcode known to the user.

Claim 45 (Previously presented): The method of Claim 43, wherein the login data comprises a password.

Claim 46 (Previously presented): The method of Claim 45, wherein the password comprises a passcode and the token, and wherein the passcode is known to the user.

Claim 47 (Previously presented): The method of Claim 46, wherein the password is a concatenation of the passcode and the token.

Claim 48 (Previously presented): The method of Claim 46, wherein the password is a hashed concatenation of the passcode and the token.

B1

Claim 49 (Previously presented): The method of Claim 43, further comprising generating the token.

Claim 50 (Previously presented): An access control system comprising:

a communication module configured to receive a request for a token, wherein the request is transmitted from a personal communication device as a result of an action by a user, and wherein the communication module is further configured to transmit the token to the personal communication device in response to the request;

a user token server configured to generate a valid password based at least upon the token; and

an authentication module configured to receive a submitted password in response to a request for authentication of the user, the authentication module further configured to grant access to the user if at least the submitted password matches the valid password.

Claim 51 (Previously presented): The system of Claim 50, wherein the user token server is further configured to generate the valid password based additionally upon a passcode that is known to the user.

Claim 52 (Previously presented): The system of Claim 51, wherein the valid password is a concatenation of the passcode and the token.

B1

Claim 53 (Previously presented): The system of Claim 59, wherein the user token server is further configured to generate the token.

AMENDMENTS TO THE DRAWINGS

Applicants have changed FIG. 1 on attached replacement sheet 1 of 11 and have changed FIG. 7B on attached replacement sheet 10 of 11. In particular, Applicants have incorporated the following changes into the two figures:

In FIG. 1, previously omitted reference designation 162 is added to identify the *AUTHENTICATION CONFIRMATION.*

In FIG. 7B, original reference designation 712 for the *NETWORK INTERFACE CARD* is changed to reference designation 702.

Attachments: Replacement Sheet 1 of 11 showing FIG. 1
Replacement Sheet 10 of 11 showing FIG. 7B

OIPE JC35 MAR 1 1 2004 PATENT & TRADEMARK OFFICE

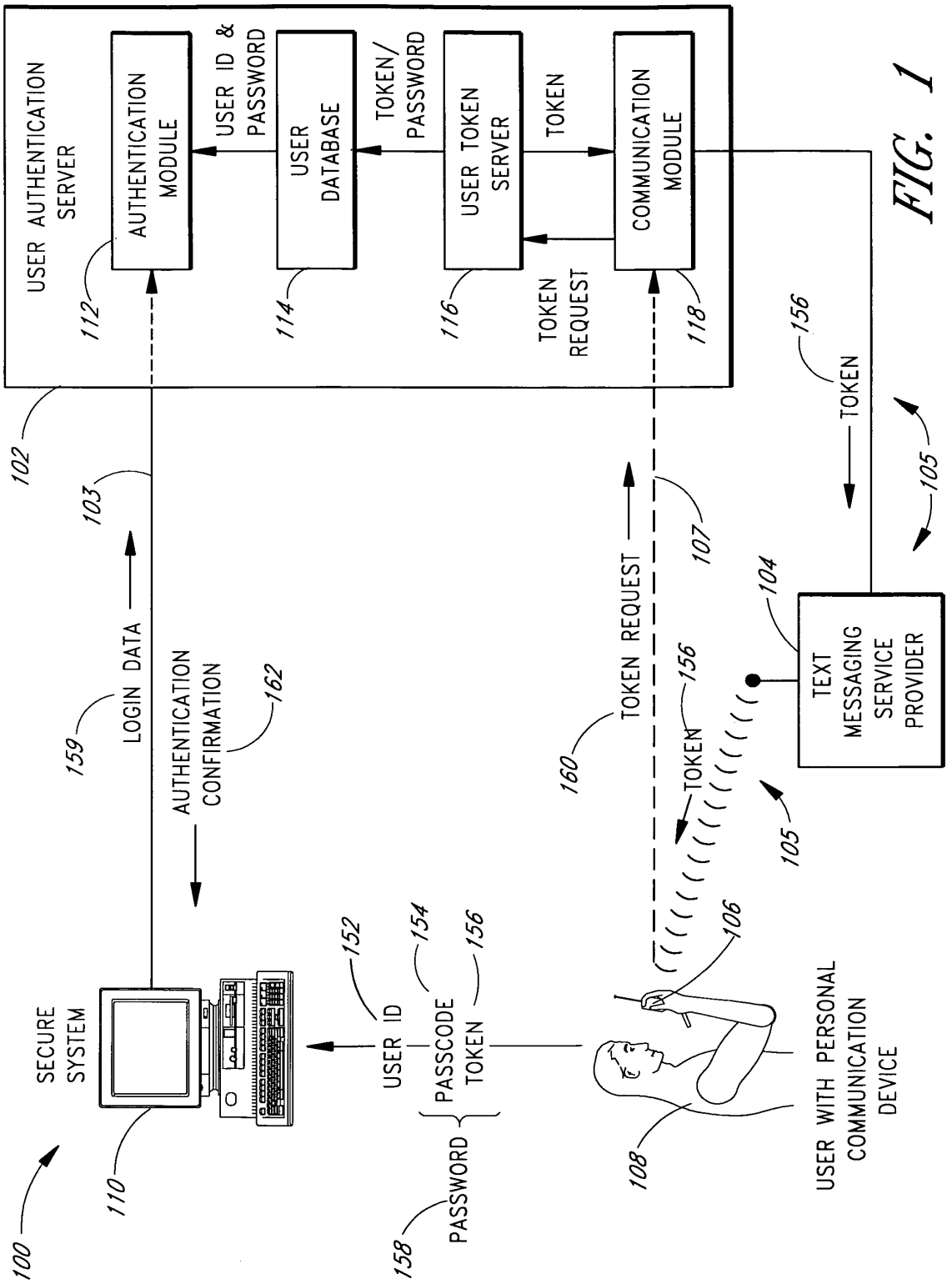


FIG. 1

OIPE JC35 MAR 1 1 2004 PATENT & TRADEMARK OFFICE

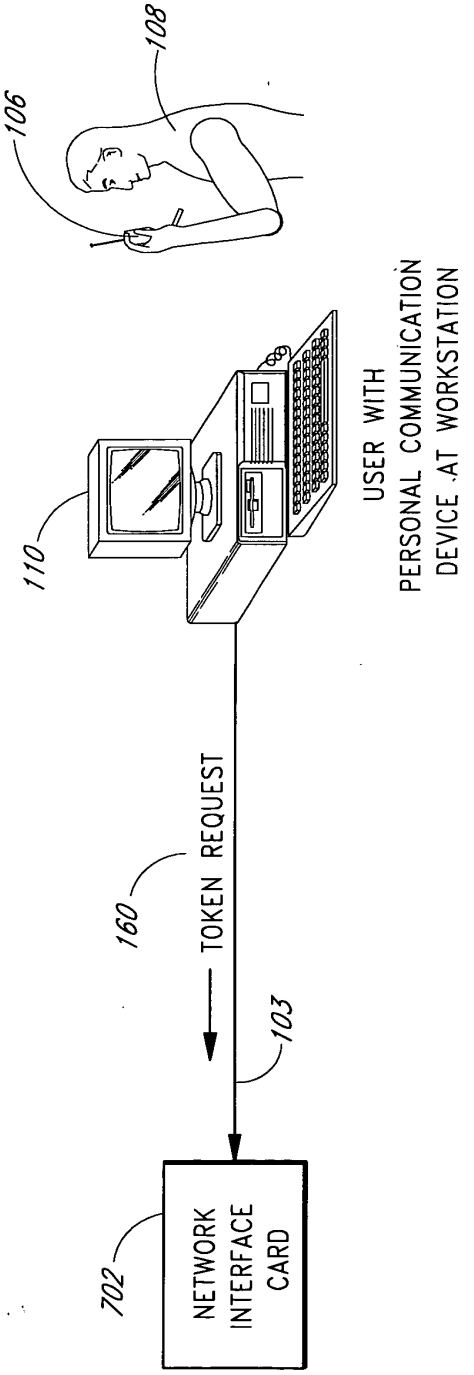


FIG. 7B

REMARKS

The foregoing amendments and drawing changes and the following remarks are response to the December 15, 2003 Office Action. Claims 28-53 are pending in the application. In the Office Action, the Examiner rejects Claims 28-53. The Examiner objects to the specification and the drawings.

Applicants have amended FIG. 1 and FIG. 7B in response to the objections to the drawings and the specification. Applicants have not amended the claims in response to the rejections; however, Applicants have amended Claim 37 to provide proper antecedent basis for *a user*.

Applicants respectfully request reconsideration of the application in view of the amendment and the drawing changes and in further view of the following remarks.

Response to the Objections to the Drawings and the Specification

In the Office Action, the Examiner objects to the drawings and the specification because reference designation 712 shown in FIG. 7B is not mentioned in the specification and because the reference designations 162 and 702 are mentioned in the specification but are not shown in the drawings.

Applicants have replaced FIG. 1 with a revised FIG. 1 on the attached replacement sheet 1 of 11. Applicants have replaced FIG. 7B with a revised FIG. 7B on the attached replacement sheet 10 of 11.

In revised FIG. 1, Applicants have added reference designation 162 to identify the *AUTHENTICATION CONFIRMATION* in accordance with the specification on page 7 at lines 15-16 and on page 11 at line 18.

In revised FIG. 7B, Applicants have changed reference designation 712 to 702 to identify the *NETWORK INTERFACE CARD* in accordance with the specification on page 16 at line 11.

The revised drawings are responsive to the objection to the drawings and are also responsive to the objection to the specification. No amendments to the specification are required.

Since the revised drawings are consistent with the original specification, Applicants respectfully submit that no new matter is introduced by the proposed drawing changes. Applicants respectfully request the Examiner to approve the revised drawings. Applicants also request the Examiner to withdraw the objection to the drawings and the objection to the specification.

Rejection of Claims 37-39 Under 35 U.S.C. § 102(b)

In the Office Action, the Examiner rejects Claims 37-39 under 35 U.S.C. §102(b) as being anticipated by Australian Patent Application No. 63545/98 to Schmitz ("Schmitz"). Applicants respectfully traverse the rejection for the following reasons.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Brothers v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the claim. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). As discussed below, Schmitz does not expressly or inherently disclose or suggest each and every element of independent Claim 37.

Figure 1 of Schmitz teaches a user sending a qualifying ID through a data input apparatus 1 to an authorization computer 2 and receiving a transaction authorization number (a "TAN") from the authorization computer 2 through a receiver 3. The user may then enter the TAN into the data input apparatus 1 for verification by the authorization computer. See page 13 at line 20 through page 14 at line 10.

Security of the system in Schmitz is accomplished by employing two separate transmission paths. The first transmission path is from the data input device 1 to the authorization computer 2 for requesting a TAN. The second transmission path is from the authorization computer 2 to the receiver 3 for providing the TAN to the user. See page 8 at lines 1-13. Thus, the **request is made through a data input device** 1 attached to the authorization computer 2 (see Fig. 1) or part of the authorization computer 2 (see page 16 at

lines 3-4). The receiver 3 for receiving the TAN, on the other hand, may be a portable device such as a pager 31 or a "handy" 32. See page 15, lines 18-25.

Unlike Claim 37, Schmitz does not teach or suggest *associating a user with a personal communication device possessed by the user, associating the user with an account, wherein an initiation of access through the account requires that the account be activated, receiving a request* ***transmitted by the personal communication device****, and in response to the receipt of the request, activating the account.* Rather, Schmitz teaches receiving a request transmitted by a data input apparatus 1 while using the receiver 3 (i.e., a personal communication device) only for receiving the TAN. Therefore, Schmitz does not teach each and every element of the invention defined in Claim 37 as required to anticipate Claim 37 under 35 U.S.C. § 102(b). Accordingly, Applicants respectfully submit that Claim 37 is patentably distinguished over Schmitz. Applicants respectfully request the Examiner to withdraw the rejection of Claim 37 under 35 U.S.C. § 102(b) and to pass Claim 37 to allowance.

Claims 38 and 39 depend from Claim 37 and further define the invention defined in Claim 37. In view of the allowability of Claim 37 and in further view of the limitations in Claims 38 and 39, Applicants respectfully submit that Claims 38 and 39 are also allowable. Applicants respectfully request that the Examiner to withdraw the rejection of Claims 38 and 39 under 35 U.S.C. § 102(b) and to pass Claims 38 and 39 to allowance.

Rejection of Claims 28-36 and 40-53 Under 35 U.S.C. § 103(a)

In the Office Action, the Examiner rejects Claims 28-36 and 40-53 under 35 U.S.C. § 103(a) as being unpatentable over Schmitz in view of Menezes, *Handbook of Applied Cryptography*, 1997, page 390. Applicants respectfully traverse this rejection for the following reasons.

Section 2143 of the M.P.E.P. states that to establish prima facie obviousness three requirements must be met:

> To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the

> art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on the Applicant's disclosure.

Applicants respectfully submit that the elements for a *prima facie* case of obviousness are not met by the proposed combination of Schmitz and Menezes because the two references do not teach or suggest all the claim limitations.

As acknowledged by the Examiner, Schmitz does not teach a method for creating a password. On page 4 of the Office Action, the Examiner states that *Menezes discloses that a password may be augmented with a random string, called a "salt," along with a hashing function, in order to make dictionary attacks less effective (see section (v)), and further notes that an entity's ID can be used as a salt.* The Examiner concludes that it would have been obvious to combine Menezes with Schmitz to obtain the claimed invention. Applicants respectfully disagree.

Menezes teaches that the salt is determined *upon initial entry* of a password into a system. Thus, only one salt exists for a corresponding password because the password is augmented by the salt *before applying the one way function.* If a new salt were generated each time a password was received for verification, the one-way function would make it impossible to compare it to the hashed password and salt created upon initial entry. Therefore, the salt taught by Menezes cannot be the same as the TAN taught by Schmitz because the security features taught by Schmitz depend on a new TAN being generated or selected each time a request is received. Further, the salt taught by Menezes is only used internally in the system verifying the password and is not transmitted to the user each time a request is received, as taught by Schmitz.

Unlike the invention defined in Claim 28, the combined references do not teach or suggest *[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.*** Thus, the invention defined in Claim 28 is not obvious in view of the proposed combination. Applicants respectfully submit that Claim 28 is patentably distinguished over Schmitz in view of Menezes. Applicants respectfully request the Examiner to withdraw the rejection of Claim 28 under 35 U.S.C. § 103(a) and to pass Claim 28 to allowance.

Claims 29-33 depend from Claim 28 and further define the invention defined in Claim 28. In view of the allowability of Claim 28 and in further view of the limitations in Claims 29-33, Applicants respectfully submit that Claims 29-33 are also patentably distinguished over the cited references. Applicants respectfully request the Examiner to withdraw the rejection of Claims 29-33 under 35 U.S.C. § 103(a).

Unlike the invention defined in Claim 34, the combined references do not teach or suggest *[a] user authentication system comprising: a user database configured to associate a user with a personal communication device possessed by the user; a control module 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; a communication module configured to transmit the token to the personal communication device; and an authentication module* ***configured to receive the password from the user.*** Thus, the invention defined in Claim 34 is not obvious in view of the proposed combination. Applicants respectfully submit that Claim 34 is patentably distinguished over Schmitz in view of Menezes. Applicants respectfully request the Examiner to withdraw the rejection of Claim 34 under 35 U.S.C. § 103(a) and to pass Claim 34 to allowance.

Claims 35 and 36 depend from Claim 34 and further define the invention defined in Claim 34. In view of the allowability of Claim 34 and in further view of the limitations in Claims 35 and 36, Applicants respectfully submit that Claims 35 and 36 are also patentably

distinguished over the cited references. Applicants respectfully request the Examiner to withdraw the rejection of Claims 35 and 36 under 35 U.S.C. § 103(a).

Unlike the invention defined in Claim 43, the combined references do not teach or suggest *[a] method of regulating access to a secure system, the method comprising: receiving a request for a token,* ***wherein the request is transmitted from a personal communication device*** *as a result of an action by a user; in response to the receipt of the request, transmitting the token to the personal communication device; receiving login data from the user in response to a request for authentication information, wherein the login data is based at least upon the token; and granting access to the secure system based at least upon the received login data.* Thus, the invention defined in Claim 43 is not obvious in view of the proposed combination. Applicants respectfully submit that Claim 43 is patentably distinguished over Schmitz in view of Menezes. Applicants respectfully request the Examiner to withdraw the rejection of Claim 43 under 35 U.S.C. § 103(a) and to pass Claim 43 to allowance.

Claims 44-49 depend from Claim 43 and further define the invention defined in Claim 43. In view of the allowability of Claim 43 and in further view of the limitations in Claims 44-49, Applicants respectfully submit that Claims 44-49 are also patentably distinguished over the cited references. Applicants respectfully request the Examiner to withdraw the rejection of Claims 44-49 under 35 U.S.C. § 103(a).

Unlike the invention defined in Claim 50, the combined references do not teach or suggest *[a]n access control system comprising: a communication module configured to receive a request for a token, wherein the request is* ***transmitted from a personal communication device*** *as a result of an action by a user, and wherein the communication module is further configured to transmit the token to the personal communication device in response to the request; a user token server configured to generate a valid password based at least upon the token; and an authentication module configured to receive a submitted password in response to a request for authentication of the user, the authentication module further configured to grant access to the user if at least the submitted password matches the valid password.* Thus, the invention defined

in Claim 50 is not obvious in view of the proposed combination. Applicants respectfully submit that Claim 50 is patentably distinguished over Schmitz in view of Menezes. Applicants respectfully request the Examiner to withdraw the rejection of Claim 50 under 35 U.S.C. § 103(a) and to pass Claim 50 to allowance.

Claims 51-53 depend from Claim 50 and further define the invention defined in Claim 50. In view of the allowability of Claim 50 and in further view of the limitations in Claims 51-53, Applicants respectfully submit that Claims 51-53 are also patentably distinguished over the cited references. Applicants respectfully request the Examiner to withdraw the rejection of Claims 51-53 under 35 U.S.C. § 103(a).

Summary

In view of the amendment to Claim 37 and the revisions to the drawings, and in further view of the foregoing discussion, Applicants respectfully submit that this application is in condition for allowance with Claims 28-53 as presented herein. Applicants respectfully request the Examiner to withdraw all objections and rejections and to pass this application with allowance with Claims 28-53.

Should the Examiner determine that additional issues may be resolved by a telephone call, the Examiner is cordially invited to contact the undersigned attorney of record so that such issues may be promptly resolved so that this application may be passed to issuance.

Respectfully submitted,
KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: MARCH 11, 2004

By: Jerry T. Sewell

Jerry T. Sewell
Registration No. 31,567
Attorney of Record
Customer No. 20,995
949-721-2849 (direct)
949-760-0404 (operator)

Attachments (two replacement sheets of drawings)

JTS-19395.DOC // 20040310/2

L Number	Hits	Search Text	DB	Time stamp
1	552	713/202.ccls.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/12 14:33
2	344	713/202.ccls. and personal	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/12 14:47
3	9	713/202.ccls. and (personal adj communication)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/12 14:47
4	10	713/202.ccls. and ((personal adj communication) ((mobile cell) adj phone) cellphone pager) and account	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/12 14:48
5	28	713/202.ccls. and ((personal adj communication) ((mobile cell) adj phone) cellphone pager) and (combin$ appen$ concaten$)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/12 14:48

L Number	Hits	Search Text	DB	Time stamp
36	46	705/74.ccls.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/13 14:12
37	29	705/74.ccls. and account	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/13 14:12
38	43	705/74.ccls. and time	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/13 14:12
39	28	705/74.ccls. and time and account	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/13 14:12
41	17	705/74.ccls. and time and account and (pass password)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/13 14:12
45	80	((create activate) adj account) and time and password	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/13 14:12
47	11	((create activate) adj account) and ((delete deactivate (de adj activate)) adj account) and password	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/13 14:12
49	15	(tempor$ adj account) and password	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/13 14:12
50	29	((tempor$ guest) adj account) and password	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/13 14:12
51	2	((tempor$ guest) adj account) same (time adj limi$)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/13 14:12
52	15	((tempor$ guest) adj account) same time	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/13 14:12
53	245	235/382.5.ccls.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/13 14:12
54	47	((tempor$ guest) adj account) and time	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/13 14:12
55	204	235/382.5.ccls. and time	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/05/13 14:12

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/519,829	03/06/2000	Sten-Olov Engberg	APRILS.001A	8563

20995 7590 05/24/2004

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	12

DATE MAILED: 05/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO 90C (Rev 10/03)

Office Action Summary	Application No.	Applicant(s)	
	09/519,829	ENGBERG ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *28-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *28-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. In response to the first office action, claim 37 has been amended. Claims 28-53 have been examined.

Drawings

2. The drawings were received on 11 March 2004. These drawings are acceptable.

Claim Objections

3. Claim 53 is objected to because of the following informalities: In the claim as recited in the most recent amendment, the claim is dependent on non-existent claim 59. It is being presumed that the claim actually depends on claim 50, as was originally recited. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4. Claims 28-31 and 43-53 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,323,146 to Glaschick.

As per claims 28-31, 43-47, and 49-53, Glaschick discloses a system wherein a user communicating with a computer system from a data station (a personal communications device). In response to a user announcement, the computer sends a random number to the data station, which then adds (concatenates) it to the password and sends it back to the computer to authenticate the user (see column 1, lines 52-68).

Regarding claim 48, the invention disclosed by Glaschick is an improvement over this system (see column 2, lines 20-40). The one-way function disclosed is a type of hash function (see column 3, lines 36-51).

5. Claims 37-39 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,226,364 to O'Neil.

As per claim 37, the user is associated with the phone and the account, and the account is activated by way of a prepaid telephone service card activation unit in response to the user request (see abstract).

As per claim 38, temporary accounts may be used (see column 19, lines 61-65). A temporary customer profile defines the limitations of the account (see column 4, lines 60-65). Temporary accounts inherently expire when they are exhausted.

As per claim 39, verification involves the user transmitting the card's serial number, which constitutes a password (see column 17, lines 16-23).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 32-36 and 40-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,226,364 to O'Neil as applied to claims 28 and 39 above, and further in view of U.S. Patent No. 5,323,146 to Glaschick.

Regarding claims 40-42, the telephone service system disclosed by O'Neil does include the claimed password protocol for logging on to the system.

Glaschick discloses the claimed protocol, as described above, and further notes that this protocol is used to prevent a privileged user from acquiring the password of a user by reading it form the memory (see column 1, lines 27-31).

Therefore it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the system of O'Neil by employing the password system disclosed by Glaschick, in order to prevent a privileged user from acquiring the password of a user by reading it form the memory.

As per claim 32, O'Neil discloses the use of cellular phones (see column 10, lines 25-56).

As per claim 33, O'Neil discloses the use of paging systems (see column 11, lines 35-48).

As per claims 34-36, a user database is used (see column 16, lines 2-20).

Response to Arguments

7. Applicant's arguments, see Paper No. 11, filed 11 March 2004, with respect to the rejections of claims 28-53 under 35 U.S.C. 102 and 35 U.S.C. 103 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new grounds of rejection are made as described above.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (703) 305-7727. The examiner can normally be reached on Monday-Thursday from 8:00 AM - 4:00 PM Eastern Time. The examiner can also be reached on alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(703) 872-9306
Hand-delivered responses should be brought to Crystal Park 2, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

MEH
May 13, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Notice of References Cited	Application/Control No. 09/519,829	Applicant(s)/Patent Under Reexamination ENGBERG ET AL.	
	Examiner Matthew Heneghan	Art Unit 2134	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-5,323,146	06-1994	Glaschick, Rainer	713/202
	B	US-6,226,364	05-2001	O'Neil, Douglas R.	379/114.2
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

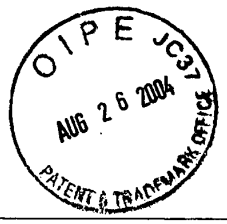
FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.



2134

PATENT

Case Docket No. APRILS.001A
Date: August 23, 2004
Page 1

In re application of	:	Sten-Olov Engberg, et al.
App. No.	:	09/519,829
Filed	:	March 6, 2000
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
Examiner	:	Matthew E. Heneghan
Art Unit	:	2134

CERTIFICATE OF MAILING

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as first-class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on

August 23, 2004
(Date)

Aaron D. Barker

Aaron D. Barker, Reg. No. 51,432

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

RECEIVED
AUG 31 2004
Technology Center 2100

Sir:

Transmitted herewith is an amendment in the above-identified application.

The fee has been calculated as shown below:

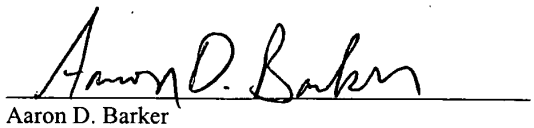
CLAIMS AS FILED

	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NO. PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE	ADDITIONAL FEE
Total Claims	26	—	26	= 0 ×	$9	= $0
Independent Claims	5	—	5	= 0 ×	$43	= $0
If application has been amended to contain multiple dependent claim(s), then add					$145	= $0
				TOTAL ADDITIONAL FEE FOR THIS AMENDMENT		$0

(X) The present application qualifies for small entity status under 37 C.F.R. § 1.27.

(X) Return prepaid postcard.

(X) Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.



Aaron D. Barker
Registration No. 51,432
Attorney of Record
Customer No. 20,995
(949) 760-0404

H:\DOCS\ADB\ADB-1625.DOC
082304

OIPE JC37
AUG 26 2004
PATENT & TRADEMARK OFFICE

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Sten-Olov Engberg et al.
Appl. No.	:	09/519,829
Filed	:	March 6, 2000
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
T.C./A.U.	:	2134
Examiner	:	Matthew E. Heneghan
Atty Docket No.	:	APRILS.001A
Confirmation No.	:	8563
Customer No.	:	20,995

RECEIVED
AUG 31 2004
Technology Center 2100

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450

AMENDMENT AND RESPONSE TO MAY 24, 2004 OFFICE ACTION

Dear Sir:

In response to the May 24, 2004 Office Action, Applicants respectfully submit the following amendments and remarks.

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 7 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application. The listing of claims present each claim with its respective status shown in parentheses.

In the following list, Claims 37 and 53 are currently amended. Claims 28-36 and 38-52 remain as previously presented.

Listing of Claims

Claim 28 (Previously presented): 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.

Claim 29 (Previously presented): The method of Claim 28, wherein the new password is generated by concatenating the token and the passcode.

Claim 30 (Previously presented): The method of Claim 28, further comprising receiving a request from the user for the token.

Claim 31 (Previously presented): The method of Claim 30, wherein the request is transmitted by the user through the personal communication device.

Claim 32 (Previously presented): The method of Claim 28, wherein the personal communication device is a mobile phone.

Claim 33 (Previously presented): The method of Claim 28, wherein the personal communication device is a pager.

Claim 34 (Previously presented): A user authentication system comprising:

a user database configured to associate a user with a personal communication device possessed by the user;

a control module 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;

a communication module configured to transmit the token to the personal communication device; and

an authentication module configured to receive the password from the user.

Claim 35 (Previously presented): The system of Claim 34, 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.

Claim 36 (Previously presented): The system of Claim 35, wherein the request is transmitted by the user through the personal communication device.

Claim 37 (Currently amended): A method of regulating access to a secure system, the method comprising:

associating a user with a personal communication device possessed by the user;

associating the user with an account, wherein an initiation of access directly to the secure system through the account requires that the account be activated;

receiving a request transmitted by the personal communication device; and

in response to the receipt of the request, activating the account.

Claim 38 (Previously presented): The method of Claim 37, further comprising deactivating the account within a predetermined amount of time after the account is activated.

Claim 39 (Previously presented): The method of Claim 37, wherein an initiation of access through the account further requires that the user supply a valid password.

Claim 40 (Previously presented): The method of Claim 39, further comprising:

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 the valid password to be the new password;

transmitting the token to the personal communication device; and

receiving the valid password from the user.

Claim 41 (Previously presented): The method of Claim 40, wherein the new password is generated by concatenating the token and the passcode.

Claim 42 (Previously presented): The method of Claim 40, wherein the token is transmitted in response to the receipt of the request.

Claim 43 (Previously presented): A method of regulating access to a secure system, the method comprising:

receiving a request for a token, wherein the request is transmitted from a personal communication device as a result of an action by a user;

in response to the receipt of the request, transmitting the token to the personal communication device;

receiving login data from the user in response to a request for authentication information, wherein the login data is based at least upon the token; and

granting access to the secure system based at least upon the received login data.

Claim 44 (Previously presented): The method of Claim 43, wherein the login data is additionally based upon a passcode known to the user.

Claim 45 (Previously presented): The method of Claim 43, wherein the login data comprises a password.

Claim 46 (Previously presented): The method of Claim 45, wherein the password comprises a passcode and the token, and wherein the passcode is known to the user.

Claim 47 (Previously presented): The method of Claim 46, wherein the password is a concatenation of the passcode and the token.

Claim 48 (Previously presented): The method of Claim 46, wherein the password is a hashed concatenation of the passcode and the token.

Claim 49 (Previously presented): The method of Claim 43, further comprising generating the token.

Claim 50 (Previously presented): An access control system comprising:

a communication module configured to receive a request for a token, wherein the request is transmitted from a personal communication device as a result of an action by a user, and wherein the communication module is further configured to transmit the token to the personal communication device in response to the request;

a user token server configured to generate a valid password based at least upon the token; and

an authentication module configured to receive a submitted password in response to a request for authentication of the user, the authentication module further configured to grant access to the user if at least the submitted password matches the valid password.

Claim 51 (Previously presented): The system of Claim 50, wherein the user token server is further configured to generate the valid password based additionally upon a passcode that is known to the user.

Claim 52 (Previously presented): The system of Claim 51, wherein the valid password is a concatenation of the passcode and the token.

Claim 53 (Currently amended): The system of Claim [[59]] 50, wherein the user token server is further configured to generate the token.

REMARKS

The foregoing amendment and the following remarks are response to the May 24, 2004 Office Action. Claims 28-53 are pending in the application. In the Office Action, the Examiner rejects Claims 28-53. The Examiner also objects to Claim 53. Applicants have amended Claims 37 and 53 herein.

Applicants respectfully request reconsideration of the application in view of the following remarks.

Response to the Claim Objections

In the Office Action, the Examiner objects to Claim 53 as being dependent on non-existent Claim 59. Applicants thank the Examiner for his careful examination of the present application and submit that the discrepancy in Claim 59 is a typographical error. Accordingly, Applicants have amended Claim 59 herein to depend from Claim 50, as was originally recited.

Rejection of Claims 28-31 and 43-53 Under 35 U.S.C. § 102(b)

In the Office Action, the Examiner rejects Claims 28-31 and 43-53 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,323,146 to Glaschick ("Glaschick"). Applicants respectfully traverse the rejection for the following reasons.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Brothers v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the claim. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). As discussed below, Glaschick does not expressly or inherently disclose or suggest each and every element of independent Claims 28, 43 and 50.

According to the Examiner, Glaschick discloses a system wherein a user communicates with a computer system using a personal communication device. See page 3 of the present Office Action. Applicants respectfully disagree. FIGS. 1 and 2 of Glaschick show a user 10 accessing a computer 14 through a data station 16 connected thereto. In a one-time procedure

(i.e., password announcement), the user 10 stores a password in a confidential file 12 of the computer 14. "If the user subsequently wants to call up a service of the computer 14 **over one of the data stations connected with it** his connection privilege is examined (authentication)." Column 4, lines 12-15 (emphasis added). Thus, the data station 16 is a connected terminal of the overall system and is not a personal communication device.

Unlike the invention defined in Claim 28, Glaschick does not disclose, teach or suggest *[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.* Rather, Glaschick is silent on using a personal communication device possessed by a user. Accordingly, Applicants respectfully submit that Claim 28 is patentably distinguished over Glaschick. Applicants respectfully request the Examiner to withdraw the rejection of Claim 28 under 35 U.S.C. § 102(b) and to pass Claim 28 to allowance.

Claims 29-31 depend from Claim 28 and further define the invention defined in Claim 28. In view of the allowability of Claim 28 and in further view of the limitations in Claims 29-31, Applicants respectfully submit that Claims 29-31 are also patentably distinguished over Glaschick. Applicants respectfully request the Examiner to withdraw the rejection of Claims 29-31.

Unlike the invention defined in Claim 43, the combined references also do not teach or suggest *[a] method of regulating access to a secure system, the method comprising: receiving a request for a token,* ***wherein the request is transmitted from a personal communication device*** *as a result of an action by a user; in response to the receipt of the request,* ***transmitting the token to the personal communication device****; receiving login data from the user in response to a request for authentication information, wherein the login data is based at least upon the token; and granting access to the secure system based at least upon the received login data.* Thus,

Applicants respectfully submit that Claim 43 is patentably distinguished over Glaschick and respectfully request the Examiner to withdraw the rejection of Claim 43.

Claims 44-49 depend from Claim 43 and further define the invention defined in Claim 43. In view of the allowability of Claim 43 and in further view of the limitations in Claims 44-49, Applicants respectfully submit that Claims 44-49 are also patentably distinguished over Glaschick. Applicants respectfully request the Examiner to withdraw the rejection of Claims 44-49.

Unlike the invention defined in Claim 50, the combined references also do not teach or suggest *[a]n access control system comprising: a communication module configured to receive a request for a token, wherein the request is* ***transmitted from a personal communication device*** *as a result of an action by a user, and wherein the communication module is further configured to* ***transmit the token to the personal communication device*** *in response to the request; a user token server configured to generate a valid password based at least upon the token; and an authentication module configured to receive a submitted password in response to a request for authentication of the user, the authentication module further configured to grant access to the user if at least the submitted password matches the valid password.* Accordingly, Applicants respectfully submit that Claim 50 is patentably distinguished over Glaschick respectfully request the Examiner to withdraw the rejection of Claim 50.

Claims 51-53 depend from Claim 50 and further define the invention defined in Claim 50. In view of the allowability of Claim 50 and in further view of the limitations in Claims 51-53, Applicants respectfully submit that Claims 51-53 are also patentably distinguished over Glaschick. Applicants respectfully request the Examiner to withdraw the rejection of Claims 51-53.

Rejection of Claims 37-39 Under 35 U.S.C. § 102(e)

In the Office Action, the Examiner rejects Claims 37-39 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,226,364 to O'Neil ("O'Neil"). Applicants respectfully traverse this rejection for the following reasons.

O'Neil teaches using a prepaid phone card to allow a user to make a cellular telephone call. The user deposits the face value of the prepaid phone card into an account by entering the serial number printed on the prepaid phone card. The account is associated with a directory number. See column 20, lines 42-62. During subsequent cellular phone calls, the system taught by O'Neil tracks the charges to the prepaid balance in the account and determines when the prepaid balance becomes exhausted. See column 21, lines 50-67. However, Applicants respectfully submit that the prepaid phone card billing and tracking system taught by O'Neil is unrelated to any of the claims in the present application.

Unlike Claim 37 as amended herein, O'Neil does not teach or suggest *[a] method of regulating access to a secure system, the method comprising: associating a user with a personal communication device possessed by the user; associating the user with an account, wherein an initiation of* ***access directly to the secure system*** *through the account requires that the account be activated, receiving a request transmitted by the personal communication device, and in response to the receipt of the request, activating the account.* Rather, O'Neil teaches accessing cellular phone service through a cellular phone. In contrast to O'Neil, Claim 37 teaches receiving a request transmitted by a personal communication device to initiate access **directly** to the secure system (i.e., not through the personal communication device). Therefore, O'Neil does not teach each and every element of the invention defined in Claim 37 as required to anticipate Claim 37 under 35 U.S.C. § 102(e). Accordingly, Applicants respectfully submit that Claim 37 is patentably distinguished over O'Neil. Applicants respectfully request the Examiner to withdraw the rejection of Claim 37 under 35 U.S.C. § 102(e) and to pass Claim 37 to allowance.

Claims 38 and 39 depend from Claim 37 and further define the invention defined in Claim 37. In view of the allowability of Claim 37 and in further view of the limitations in Claims 38 and 39, Applicants respectfully submit that Claims 38 and 39 are also allowable. Applicants respectfully request that the Examiner to withdraw the rejection of Claims 38 and 39 under 35 U.S.C. § 102(e) and to pass Claims 38 and 39 to allowance.

Rejection of Claims 32-36 and 40-42 Under 35 U.S.C. § 103(a)

In the Office Action, the Examiner rejects Claims 32-36 and 40-42 under 35 U.S.C. § 103(a) as being unpatentable over O'Neil in view of Glaschick. Applicants respectfully traverse this rejection for the following reasons.

Section 2143 of the M.P.E.P. states that to establish prima facie obviousness three requirements must be met:

> To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on the Applicant's disclosure.

Applicants respectfully submit that the elements for a *prima facie* case of obviousness are not met by the proposed combination of O'Neil and Glaschick. Specifically, there is no suggestion or motivation to combine the references, and the references (either individually or when combined) do not teach or suggest all the claim limitations.

There is no suggestion or motivation in the references to combine the teachings of O'Neil and Glaschick. As discussed above, Glaschick teaches a method of authenticating a user of a data station connected to a computer system by exchanging information between the data station and the computer system. However, Glaschick does not suggest a need for using a personal communications device as part of its system. Further, the prepaid telephone card billing and tracking system taught by O'Neil is completely unrelated to the subject matter taught in Glaschick. While, as the Examiner points out, O'Neil teaches receiving a unique serial number and barcode as printed on the prepaid phone card in order to prevent dissemination of counterfeit cards and card information (see column 17, lines 15-22), O'Neil does not suggest or provide any

motivation for implementing the elaborate authentication system in Glaschick including multiple exchanges of hashed passwords. O'Neil does not even suggest a need for additional security measures.

Rather, it appears that the Examiner has impermissibly used hindsight derived from the teachings in the present application, and not the teachings in the prior art. See In re Dembiczak, 175 F.3d 994, 999 (Fed. Cir. 1999) (holding the Board impermissibly used hindsight in determining obviousness). In Dembiczak, the Federal Circuit reiterated that a determination of obviousness cannot simply rely on the inventor's disclosure as a "blueprint" without evidence of a suggestion, teaching or motivation in the prior art. Id. Thus, there is not a *prima facie* case of obviousness.

Even if O'Neil and Glaschick were to be combined, which they cannot be, they would not teach or suggest each claim limitation of independent Claim 34. Unlike the invention defined in Claim 34, the combined references do not teach or suggest *[a] user authentication system comprising: a user database configured to associate a user with a personal communication device possessed by the user; a control module 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; a communication module configured to* ***transmit the token to the personal communication device****; and an authentication module configured to receive the password from the user.* Rather, both O'Neil and Glaschick are silent as to the subject matter of Claim 34. Thus, the invention defined in Claim 34 is not obvious in view of the proposed combination. Applicants respectfully submit that Claim 34 is patentably distinguished over O'Neil in view of Glaschick. Applicants respectfully request the Examiner to withdraw the rejection of Claim 34 under 35 U.S.C. § 103(a) and to pass Claim 34 to allowance.

Claims 35 and 36 depend from Claim 34 and further define the invention defined in Claim 34. As discussed above, Claims 32-33 and 40-42 also depend from allowable independent claims. In view of the allowability of the respective independent claims and in further view of

the limitations in Claims 32-33, 35-36 and 40-42, Applicants respectfully submit that Claims 32-33, 35-36 and 40-42 are also patentably distinguished over the cited references. Therefore, Applicants respectfully submit that Claims 32-33, 35-36 and 40-42 are also allowable. Applicants respectfully request the Examiner to withdraw the rejection of Claims 32-33, 35-36 and 40-42 under 35 U.S.C. § 103(a).

Summary

In view of the foregoing discussion, Applicants respectfully submit that this application is in condition for allowance with Claims 28-53 as presented herein. Applicants respectfully request the Examiner to withdraw all objections and rejections and to pass this application with allowance with Claims 28-53.

Should the Examiner determine that additional issues may be resolved by a telephone call, the Examiner is cordially invited to contact the undersigned attorney of record so that such issues may be promptly resolved so that this application may be passed to issuance.

Respectfully submitted,
KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: August 23, 2004

By: Aaron D. Barker

Aaron D. Barker
Registration No. 51,432
Attorney of Record
Customer No. 20,995
949-721-2942 (direct)
949-760-0404 (operator)

H:\DOCS\ADB\ADB-1594.DOC
081404

PATENT APPLICATION FEE DETERMINATION RECORD
Effective December 29, 1999

Application or Docket Number: 9/519,829

CLAIMS AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA
BASIC FEE		
TOTAL CLAIMS	37 minus 20=	* 7
INDEPENDENT CLAIMS	4 minus 3 =	* 1
MULTIPLE DEPENDENT CLAIM PRESENT		

SMALL ENTITY TYPE ☐ RATE	FEE	OR	OTHER THAN SMALL ENTITY RATE	FEE
	345.00	OR		690.00
X$ 9=		OR	X$18=	126
X39=		OR	X78=	78
+130=		OR	+260=	
TOTAL		OR	TOTAL	984

* If the difference in column 1 is less than zero, enter "0" in column 2

CLAIMS AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 26	Minus	** 27	=
Independent	* 5	Minus	*** 4	= 1
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

SMALL ENTITY RATE	ADDITIONAL FEE	OR	OTHER THAN SMALL ENTITY RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X39= 40	40	OR	X78=	
+130=		OR	+260=	
TOTAL ADDIT. FEE	40	OR	TOTAL ADDIT. FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 26	Minus	** 26	= —
Independent	* 5	Minus	*** 5	= —
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

RATE	ADDITIONAL FEE	OR	RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X39=		OR	X78=	
+130=		OR	+260=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 26	Minus	** 26	= —
Independent	* 5	Minus	*** 5	= —
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

RATE	ADDITIONAL FEE	OR	RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X39=		OR	X78=	
+130=		OR	+260=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
***If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

FORM PTO-875
(Rev. 12/99)

Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
U.S. GPO: 2000-483-433/28044

49

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/519,829	03/06/2000	Sten-Olov Engberg	APRILS.001A	8563

20995 7590 02/07/2005

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 02/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Office Action Summary	Application No.	Applicant(s)	
	09/519,829	ENGBERG ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *28-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *28-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. In response to the first office action, claim 37 has been amended. Claims 28-53 have been examined.

Claim Objections

2. All previous claim objections are withdrawn.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000.

Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

3. Claims 28-31 and 43-53 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,323,146 to Glaschick.

As per claims 28-31, 43-47, and 49-53, Glaschick discloses a system wherein a user communicating with a computer system from a data station (a personal communications device). In response to a user announcement, the computer sends a random number to the data station, which then adds (concatenates) it to the password and sends it back to the computer to authenticate the user (see column 1, lines 52-68).

Regarding claim 48, the invention disclosed by Glaschick is an improvement over this system (see column 2, lines 20-40). The one-way function disclosed is a type of hash function (see column 3, lines 36-51).

4. Claims 37-39 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,226,364 to O'Neil.

As per claim 37, the user is associated with the phone and the account, and the account is activated by way of a prepaid telephone service card activation unit in response to the user request (see abstract). This process enables use of a telephone system, which, since it denies access to unauthorized users (see column 9, lines 7-28), constitutes a "secure system."

As per claim 38, temporary accounts may be used (see column 19, lines 61-65). A temporary customer profile defines the limitations of the account (see column 4, lines 60-65). Temporary accounts inherently expire when they are exhausted.

As per claim 39, verification involves the user transmitting the card's serial number, which constitutes a password (see column 17, lines 16-23).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 32-36 and 40-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,226,364 to O'Neil as applied to claim 39 above, and further in view of U.S. Patent No. 5,323,146 to Glaschick.

Regarding claims 40-42, the telephone service system disclosed by O'Neil does include the claimed password protocol for logging on to the system.

Glaschick discloses the claimed protocol, as described above, and further notes that this protocol is used to prevent a privileged user from acquiring the password of a user by reading it form the memory (see column 1, lines 27-31).

Therefore it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the system of O'Neil by employing the password system disclosed by Glaschick, in order to prevent a privileged user from acquiring the password of a user by reading it from the memory.

As per claim 32, O'Neil discloses the use of cellular phones (see column 10, lines 25-56).

As per claim 33, O'Neil discloses the use of paging systems (see column 11, lines 35-48).

As per claims 34-36, a user database is used (see column 16, lines 2-20).

Response to Arguments

6. Applicant's arguments filed 26 August 2004 have been fully considered but they are not persuasive.

Regarding Applicant's argument that Glaschick does not disclose a personal communications device (see Remarks, filed 26 August 2004), the 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.

Regarding Applicant's arguments that amended claim 37 is not anticipated by O'Neil, the explanation of the rejection above has been changed in view of Applicant's amendment.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, one skilled in the art would recognize that the motivation supplied by Glaschick would apply to *any* computerized system having authentication. The fact that O'Neil does not recognize the vulnerability that Glaschick's protocol resolves does not mean that the problem does not

exist; one skilled in the art could therefore reasonably be expected to combine the two pieces of art.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday, Tuesday, Thursday, and Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(703) 872-9306

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH
January 28, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Index of Claims

Application No.	Applicant(s)	
09/519,829	ENGBERG ET AL.	
Examiner	**Art Unit**	
Matthew Heneghan	2134	

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claim		Date								
Final	Original	1/28/05								
	1	-								
	2	-								
	3	-								
	4	-								
	5	-								
	6	-								
	7	-								
	8	-								
	9	-								
	10	-								
	11	-								
	12	-								
	13	-								
	14	-								
	15	-								
	16	-								
	17	-								
	18	-								
	19	-								
	20	-								
	21	-								
	22	-								
	23	-								
	24	-								
	25	-								
	26	-								
	27	-								
	28	√								
	29	√								
	30	√								
	31	√								
	32	√								
	33	√								
	34	√								
	35	√								
	36	√								
	37	√								
	38	√								
	39	√								
	40	√								
	41	√								
	42	√								
	43	√								
	44	√								
	45	√								
	46	√								
	47	√								
	48	√								
	49	√								
	50	√								

Claim		Date								
Final	Original	1/28/05								
	51	√								
	52	√								
	53	√								
	54									
	55									
	56									
	57									
	58									
	59									
	60									
	61									
	62									
	63									
	64									
	65									
	66									
	67									
	68									
	69									
	70									
	71									
	72									
	73									
	74									
	75									
	76									
	77									
	78									
	79									
	80									
	81									
	82									
	83									
	84									
	85									
	86									
	87									
	88									
	89									
	90									
	91									
	92									
	93									
	94									
	95									
	96									
	97									
	98									
	99									
	100									

Claim		Date								
Final	Original									
	101									
	102									
	103									
	104									
	105									
	106									
	107									
	108									
	109									
	110									
	111									
	112									
	113									
	114									
	115									
	116									
	117									
	118									
	119									
	120									
	121									
	122									
	123									
	124									
	125									
	126									
	127									
	128									
	129									
	130									
	131									
	132									
	133									
	134									
	135									
	136									
	137									
	138									
	139									
	140									
	141									
	142									
	143									
	144									
	145									
	146									
	147									
	148									
	149									
	150									

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/519,829	03/06/2000	Sten-Olov Engberg	APRILS.001A	8563

20995 7590 05/04/2005

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Interview Summary	Application No.	Applicant(s)	
	09/519,829	ENGBERG ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Matthew Heneghan*. (3)*Aaron Barker*.

(2) *Stephen Jensen*. (4)_____.

Date of Interview: *28 April 2005*.

Type: a)☒ Telephonic b)☐ Video Conference
c)☐ Personal [copy given to: 1)☐ applicant 2)☐ applicant's representative]

Exhibit shown or demonstration conducted: d)☐ Yes e)☐ No.
If Yes, brief description: _____.

Claim(s) discussed: *32 and 38*.

Identification of prior art discussed: *Glaschik, O'Neill*.

Agreement with respect to the claims f)☐ was reached. g)☒ was not reached. h)☐ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: *Attorney Jensen suggested possible amendments to the claims that might bring the application into allowability. No agreement was reached*.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN ONE MONTH FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Examiner Note: You must sign this form unless it is an Attachment to a signed Office action.

Examiner's signature, if required

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)
In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

PTOL-413A (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 09/519829 First Named Applicant: Engberg, Sten-Olov
Examiner: M. Heneghan Art Unit: 2134 Status of Application: Rejected-Final

Tentative Participants:
(1) Stephen Jensen (2) Aaron Barker
(3) _____ (4) _____

Proposed Date of Interview: Thurs, 4-28-05 **Proposed Time:** 10AM/PST 1PM/EST

Type of Interview Requested:
(1) [X] Telephonic (2) [ ] Personal (3) [ ] Video Conference

Exhibit To Be Shown or Demonstrated: [ ] YES [X] NO
If yes, provide brief description: _____

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1) Rej 102	28-31; 43-53	Glaschik	[ ]	[ ]	[ ]
(2) Rej 103	32-36	O'Neill & Glaschik	[ ]	[ ]	[ ]
(3) _____	_____	_____	[ ]	[ ]	[ ]
(4) _____	_____	_____	[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached

Brief Description of Arguments to be Presented:
Clarifying amendments regarding separation of authenticated network and password receipt device, and inclusion of dependent Claims 32 and 38 into independent claims

An interview was conducted on the above-identified application on 4/28/05.
NOTE: This form should be completed by applicant and submitted to the examiner in advance of the interview (see MPEP § 713.01).
This application will not be delayed from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible.

Stephen C. Jensen
Applicant/Applicant's Representative Signature

Examiner/SPE Signature

Stephen C. Jensen
Typed/Printed Name of Applicant or Representative

35,556
Registration Number, if applicable

This collection of information is required by 37 CFR 1.133. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

OIPE
MAY 1 2 2005
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Sten-Olov Engberg et al.
Appl. No.	:	09/519,829
Filed	:	March 6, 2000
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
Examiner	:	Matthew E. Heneghan
Group Art Unit	:	2134

CERTIFICATE OF MAILING

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as first-class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on

9 May 2005
(Date)

Stephen C. Jensen
Stephen C. Jensen, Reg. No. 35,556

AMENDMENT AND RESPONSE TO FINAL OFFICE ACTION

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The following amendments and remarks are filed in response to the Final Office Action mailed February 7, 2005. As May 7, 2005 was a Saturday, Applicants respectfully submit the following amendments and remarks on or before three months from the mailing date of the Final Office Action.

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Summary of Interview begins on page 4 of this paper.

Remarks/Arguments begin on page 5 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application. The listing of claims present each claim with its respective status shown in parentheses.

In the following list, Claims 28 and 34 are currently amended, Claims 30-31 and 37-53 are canceled, and Claims 29, 32-33 and 35-36 remain as previously presented.

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.

Claim 29 (Previously presented): The method of Claim 28, wherein the new password is generated by concatenating the token and the passcode.

Claims 30-31 (Canceled)

Claim 32 (Previously presented): The method of Claim 28, wherein the personal communication device is a mobile phone.

Claim 33 (Previously presented): The method of Claim 28, wherein the personal communication device is a pager.

Claim 34 (Previously presented): A user authentication system comprising:

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;

a control module 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;

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

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.

Claim 35 (Previously presented): The system of Claim 34, 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.

Claim 36 (Previously presented): The system of Claim 35, wherein the request is transmitted by the user through the personal communication device.

Claims 37-53 (Canceled)

SUMMARY OF INTERVIEW

Applicants thank the Examiner for the telephone interview with the Applicants' undersigned attorney. During the interview, Applicants discussed the prior art and proposed amendments to the claims, to point out the separation of the network on which the user is being authenticated to access the user's account, and the personal communication device on the cell phone network. The amendments herein reflect the proposed amendments as discussed.

REMARKS

The Final Office Action mailed February 7, 2005 has been received and reviewed. This Amendment and Response to Final Office Action accompanies a Request for Continued Examination. Applicants have amended Claims 28 and 34 and have canceled Claims 30-31 and 37-53 without prejudice or disclaimer. Accordingly, Claims 28-29 and 32-36 remain pending for consideration. Applicants respectfully request reconsideration of the application as amended herein.

Rejection of Claims 28-31 and 43-53 Under 35 U.S.C. § 102(b)

In the Office Action, the Examiner rejects Claims 28-31 and 43-53 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,323,146 to Glaschick ("Glaschick"). Applicants respectfully traverse the rejection for the following reasons.

Independent Claim 28 has been amended herein to reflect amendments proposed in an interview with the Examiner. Applicants respectfully submit that Claim 28 is patentable over Glaschick and request that the rejection be withdrawn. Applicants also respectfully submit that Claim 29 is patentable, among other reasons, as depending from Claim 28.

Claims 31 and 43-53 have been canceled without prejudice herein, mooting the rejection of these claims.

Rejection of Claims 37-39 Under 35 U.S.C. § 102(e)

In the Office Action, the Examiner rejects Claims 37-39 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,226,364 to O'Neil ("O'Neil"). Applicants respectfully disagree with the Examiner. However, Applicants have canceled Claims 37-39, mooting this rejection.

Rejection of Claims 32-36 and 40-42 Under 35 U.S.C. § 103(a)

In the Office Action, the Examiner rejects Claims 32-36 and 40-42 under 35 U.S.C. § 103(a) as being unpatentable over O'Neil in view of Glaschick. Applicants respectfully traverse this rejection for the following reasons.

Independent Claim 34 has been amended herein to reflect amendments proposed in an interview with the Examiner. Applicants respectfully submit that Claim 34 is patentable over O'Neil in view of Glaschick and request that the rejection be withdrawn. Applicants also

respectfully submit that Claims 35 and 36 are patentable, among other reasons, as depending from Claim 34. Claims 32 and 33 are patentable, among other reasons, as depending from Claim 28, which is patentable.

Claims 40-42 have been canceled without prejudice herein, mooting the rejection of these claims.

In conclusion, Claims 28-29 and 32-36 are believed to be in condition for allowance, and an early notification thereof is respectfully solicited. Should the Examiner determine that additional issues may be resolved by a telephone call, the Examiner is invited to contact the undersigned so that such issues may be promptly resolved and the case passed to issuance.

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 9 May 2005

By: _____

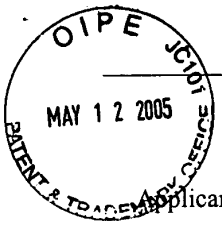
Stephen C. Jensen
Registration No. 35,556
Attorney of Record
Customer No. 20,995
(949) 760-0404

1702981
050905

Docket No.: APRILS.001A

May 9, 2005
Page 1 of 2

Rce
2134
TW



Please Direct All Correspondence to Customer Number **20995**

REQUEST FOR CONTINUED EXAMINATION

Applicant	:	Sten-Olov Engberg, et al.
App. No	:	09/519,829
Filed	:	March 6, 2000
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
Examiner	:	Matthew E. Heneghan
Art Unit	:	2134

CERTIFICATE OF MAILING

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as first-class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on

May 9, 2005
(Date)

Stephen C. Jensen, Reg. No. 35,556

Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This Request for Continued Examination (RCE) is being made as follows:

1. Submission Required under 37 CFR 1.114:

(X) Enclosed:

(X) Amendment/Reply in 6 pages.

(X) Return Postcard.

2. Fees:

FEE CALCULATION				
FEE TYPE		**FEE CODE**	**CALCULATION**	**TOTAL**
RCE Fee		2801 ($395)		$395
Suspension of Action		1463 ($130)		$0
Total Claims	5 - 26 = 0	2202 ($25)	0 x 25 =	$0
Independent Claims	2 - 6 = 0	2201 ($100)	0 x 100 =	$0
			TOTAL FEE DUE	**$395**

3. Payment:

(X) Check in the amount of $395 to cover the above fees.

05/13/2005 AWONDAF1 00000033 09519829

01 FC:2801 395.00 OP

Please Direct All Correspondence to Customer Number **20995**

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Respectfully submitted,
KNOBBE MARTENS OLSON & BEAR LLP

Dated: May 9, 2005

Stephen C. Jensen
Registration No. 35,556
Attorney of Record
Customer No. 20,995
(949) 760-0404

1703757/ap
050905

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 1996

Application or Docket Number: 09/519,829

CLAIMS AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA
BASIC FEE		
TOTAL CLAIMS	27 minus 20 =	* 7
INDEPENDENT CLAIMS	4 minus 3 =	* 1
MULTIPLE DEPENDENT CLAIM PRESENT		

SMALL ENTITY RATE	SMALL ENTITY FEE	OR	OTHER THAN SMALL ENTITY RATE	OTHER THAN SMALL ENTITY FEE
	~~345~~ 385.00	OR		~~770.00~~
x$~~11~~ 9 =	63	OR	x$~~22~~ 18 =	
~~40~~ 39 =	39	OR	x80=	
+130=		OR	+260=	
TOTAL	~~447~~	OR	TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2

5/12/05

CLAIMS AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 7	Minus	** 26	= 0
Independent	* 2	Minus	*** 5	= 0
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

SMALL ENTITY RATE	SMALL ENTITY ADDITIONAL FEE	OR	OTHER THAN SMALL ENTITY RATE	OTHER THAN SMALL ENTITY ADDITIONAL FEE
x$11=		OR	x$22=	
x40=		OR	x80=	
+130=		OR	+260=	
TOTAL ADDIT. FEE	0	OR	TOTAL ADDIT. FEE	0

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

SMALL ENTITY RATE	SMALL ENTITY ADDITIONAL FEE	OR	OTHER THAN SMALL ENTITY RATE	OTHER THAN SMALL ENTITY ADDITIONAL FEE
x$11=		OR	x$22=	
x40=		OR	x80=	
+130=		OR	+260=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				

SMALL ENTITY RATE	SMALL ENTITY ADDITIONAL FEE	OR	OTHER THAN SMALL ENTITY RATE	OTHER THAN SMALL ENTITY ADDITIONAL FEE
x$11=		OR	x$22=	
x40=		OR	x80=	
+130=		OR	+260=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in colum

FORM PTO-875

BEST AVAILABLE COPY

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

20995 7590 08/08/2005

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 08/08/2005

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/519,829	03/06/2000	Sten-Olov Engberg	APRILS.001A	8563

TITLE OF INVENTION: USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$700	$0	$700	11/08/2005

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE REFLECTS A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE APPLIED IN THIS APPLICATION. THE PTOL-85B (OR AN EQUIVALENT) MUST BE RETURNED WITHIN THIS PERIOD EVEN IF NO FEE IS DUE OR THE APPLICATION WILL BE REGARDED AS ABANDONED.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL should be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). Even if the fee(s) have already been paid, Part B - Fee(s) Transmittal should be completed and returned. If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 07/05) Approved for use through 04/30/2007.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571) 273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

20995 7590 08/08/2005

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/519,829	03/06/2000	Sten-Olov Engberg	APRILS.001A	8563

TITLE OF INVENTION: USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$700	$0	$700	11/08/2005

EXAMINER	ART UNIT	CLASS-SUBCLASS
HENEGHAN, MATTHEW E	2134	713-185000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are enclosed:
- ☐ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s):
- ☐ A check in the amount of the fee(s) is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Director is hereby authorized by charge the required fee(s), or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

The Director of the USPTO is requested to apply the Issue Fee and Publication Fee (if any) or to re-apply any previously paid issue fee to the application identified above.
NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/519,829	03/06/2000	Sten-Olov Engberg	APRILS.001A	8563

20995 7590 08/08/2005

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 08/08/2005

Determination of Patent Term Extension under 35 U.S.C. 154 (b)
(application filed after June 7, 1995 but prior to May 29, 2000)

The Patent Term Extension is 0 day(s). Any patent to issue from the above-identified application will include an indication of the 0 day extension on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Extension is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571) 272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at (703) 305-8283.

PTOL-85 (Rev. 07/05) Approved for use through 04/30/2007.

Notice of Allowability	Application No.	Applicant(s)	
	09/519,829	ENGBERG ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the amendment filed 12 May 2005*.

2. ☒ The allowed claim(s) is/are *28,29 and 32-36*.

3. ☒ The drawings filed on *11 March 2004* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *7/21/05* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Claim 34 is amended as follows:

After the first line, a limitation is added, "a computer processor;"

The limitation beginning on the original fifth line is amended to "a control module executed on the computer processor configured to create..."

Authorization for this examiner's amendment was given in a telephone interview with Attorney Stephen Jensen on 21 July 2005.

7/21/05

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12 May 2005 has been entered.

2. In response to the first office action, claims 28 and 34 have been amended and claims 30, 31, and 37-53 have been cancelled. Claims 28, 29, and 30-36 have been examined.

Allowable Subject Matter

3. Claims 28, 29, and 32-36 are allowed.

4. The following is an examiner's statement of reasons for allowance:

In each independent claim, no art could be found wherein the transaction for determining the password in the setting up of a new calling-card-derived temporary

network account is performed entirely over a connection other than that used by eventual network account.

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. This is also the case in as well as U.S. Patent No. 6,075,860 to Ketcham and U.S. Patent No. 5,949,882 to Angelo.

U.S. Patent No. 5,265,155 to Castro and U.S. Patent No. 6,795,852 to Kleinrock et al. disclose the construction of an account using an external connection, but do not suggest any password exchange.

U.S. Patent No. 5,749,075 to Toader et al. discloses the use of a temporary account with a PIN, but the PIN is initially issued and not changeable.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH

July 21, 2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	09/519,829	ENGBERG ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

All Participants:

(1) *Matthew Heneghan*.

(2) *Attorney Stephen Jensen*.

Status of Application: *Pending*

(3) _____.

(4) _____.

Date of Interview: *21 July 2005*

Time: *2:00 PM EDT*

Type of Interview:
- ☒ Telephonic
- ☐ Video Conference
- ☐ Personal (Copy given to: ☐ Applicant ☐ Applicant's representative)

Exhibit Shown or Demonstrated: ☐ Yes ☒ No
If Yes, provide a brief description:

Part I.

Rejection(s) discussed:
N/A

Claims discussed:
34

Prior art documents discussed:
N/A

Part II.

SUBSTANCE OF INTERVIEW DESCRIBING THE GENERAL NATURE OF WHAT WAS DISCUSSED:
See Continuation Sheet

Part III.

☒ It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview directly resulted in the allowance of the application. The examiner will provide a written summary of the substance of the interview in the Notice of Allowability.

☐ It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview did not result in resolution of all issues. A brief summary by the examiner appears in Part II above.

7/21/05

(Examiner/SPE Signature) (Applicant/Applicant's Representative Signature – if appropriate)

Continuation of Substance of Interview including description of the general nature of what was discussed: The Examiner communicated that claim 34 as submitted was non-statutory under 35 U.S.C. 101 because it taught to functional descriptive material that was not tangibly embodied. The Examiner proposed an amendment to claim 34 to bring it to a state of allowance, to which Attorney Jensen agreed..

Notice of References Cited	Application/Control No. 09/519,829	Applicant(s)/Patent Under Reexamination ENGBERG ET AL.	
	Examiner Matthew Heneghan	Art Unit 2134	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
X	A	US-5,265,155	11-1993	Castro, Peter D.	379/114.2
X	B	US-5,749,075	05-1998	Toader et al.	705/14
X	C	US-5,949,882	09-1999	Angelo, Michael F.	713/185
X	D	US-6,075,860	06-2000	Ketcham, Carl	713/185
X	E	US-6,795,852	09-2004	Kleinrock et al.	709/220
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Issue Classification	Application/Control No.	Applicant(s)/Patent under Reexamination	
	09/519,829	ENGBERG ET AL.	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

ISSUE CLASSIFICATION

ORIGINAL					CROSS REFERENCE(S)							
CLASS				SUBCLASS	CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)						
713				185	379	114.2						
INTERNATIONAL CLASSIFICATION					709	219						
G	0	7	F	07/10	713	183	201	202				
H	0	4	L	09/32								
H	0	4	L	12/14								
H	0	4	M	15/00								
				/								

M. Heneghan 7/19/05
(Assistant Examiner) (Date)

Brenda Harrison
(Legal Instruments Examiner) (Date)

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100
(Primary Examiner) (Date) 7/22/05

Total Claims Allowed: 7

O.G. Print Claim(s)	O.G. Print Fig.
28	1

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		31		61		91		121		151		181
	2	3	32		62		92		122		152		182
	3	4	33		63		93		123		153		183
	4	5	34		64		94		124		154		184
	5	6	35		65		95		125		155		185
	6	7	36		66		96		126		156		186
	7		37		67		97		127		157		187
	8		38		68		98		128		158		188
	9		39		69		99		129		159		189
	10		40		70		100		130		160		190
	11		41		71		101		131		161		191
	12		42		72		102		132		162		192
	13		43		73		103		133		163		193
	14		44		74		104		134		164		194
	15		45		75		105		135		165		195
	16		46		76		106		136		166		196
	17		47		77		107		137		167		197
	18		48		78		108		138		168		198
	19		49		79		109		139		169		199
	20		50		80		110		140		170		200
	21		51		81		111		141		171		201
	22		52		82		112		142		172		202
	23		53		83		113		143		173		203
	24		54		84		114		144		174		204
	25		55		85		115		145		175		205
	26		56		86		116		146		176		206
	27		57		87		117		147		177		207
1	28		58		88		118		148		178		208
2	29		59		89		119		149		179		209
	30		60		90		120		150		180		210

Search Notes	Application/Control No.	Applicant(s)/Patent under Reexamination
	09/519,829	ENGBERG ET AL.
	Examiner	Art Unit
	Matthew Heneghan	2134

SEARCHED			
Class	Subclass	Date	Examiner
713	182,183, 185,202	7/18/2005	MH
379	114.2	7/19/2005	MH
709	219	7/19/2005	MH

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner
713	**182,183**	7/19/2005	**MH**
713	185,202	7/19/2005	MH
379	114.2	7/19/2005	MH
709/219		7/19/2005	MH

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
EAST, keywords: password, passcode, network, cellphone, temporary account, guest, delete, tear down, terminate, expunge,remov	7/18/2005	MH
Consulted with Pat Salce, Marc Bookbinder re 101 rejections	7/21/2005	MH

Index of Claims

Application/Control No.	Applicant(s)/Patent under Reexamination
09/519,829	ENGBERG ET AL.
Examiner	**Art Unit**
Matthew Heneghan	2134

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claim		Date
Final	Original	7/19/05
	1	
	2	
	3	
	4	
	5	
	6	
	7	
	8	
	9	
	10	
	11	
	12	
	13	
	14	
	15	
	16	
	17	
	18	
	19	
	20	
	21	
	22	
	23	
	24	
	25	
	26	
	27	
1	28	=
2	29	=
	30	
	31	
3	32	=
4	33	=
5	34	=
6	35	=
7	36	=
	37	
	38	
	39	
	40	
	41	
	42	
	43	
	44	
	45	
	46	
	47	
	48	
	49	
	50	

Claim		Date
Final	Original	
	51	
	52	
	53	
	54	
	55	
	56	
	57	
	58	
	59	
	60	
	61	
	62	
	63	
	64	
	65	
	66	
	67	
	68	
	69	
	70	
	71	
	72	
	73	
	74	
	75	
	76	
	77	
	78	
	79	
	80	
	81	
	82	
	83	
	84	
	85	
	86	
	87	
	88	
	89	
	90	
	91	
	92	
	93	
	94	
	95	
	96	
	97	
	98	
	99	
	100	

Claim		Date
Final	Original	
	101	
	102	
	103	
	104	
	105	
	106	
	107	
	108	
	109	
	110	
	111	
	112	
	113	
	114	
	115	
	116	
	117	
	118	
	119	
	120	
	121	
	122	
	123	
	124	
	125	
	126	
	127	
	128	
	129	
	130	
	131	
	132	
	133	
	134	
	135	
	136	
	137	
	138	
	139	
	140	
	141	
	142	
	143	
	144	
	145	
	146	
	147	
	148	
	149	
	150	

S972	101	((temporary guest) adj account) and (delete (tear adj down) remove)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/18 09:53
S973	4	((temporary guest) adj account) same (delete (tear adj down) remove)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/18 09:54
S974	11	((temporary guest) adj account) same (terminat$ expung$)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/18 09:58
S975	0	((temporary guest) adj account) near2 remove	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/18 09:59
S976	77	((temporary guest) adj account) and remove	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/18 10:03
S977	22	((temporary) adj account) and delete	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/18 10:03
S978	102	("5153919" "6226364" "5323146") and (password passcode pass)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/07/18 16:14
S979	241	713/182,183,185,202.ccls. and (pass password passcode) and (cellular cellphone)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/07/18 16:15
S980	117	713/182,183,185,202.ccls. and (pass password passcode) and (cellular cellphone) and account	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/07/18 16:15

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	1	"5742756".PN.	USPAT; USOCR	OR	ON	2005/07/19 09:35
L3	1	"5740361".PN.	USPAT; USOCR	OR	ON	2005/07/19 09:36
L4	1	"5602918".PN.	USPAT; USOCR	OR	ON	2005/07/19 09:36
L5	1	"5588059".PN.	USPAT; USOCR	OR	ON	2005/07/19 09:37
L6	1	"5557679".PN.	USPAT; USOCR	OR	ON	2005/07/19 09:37
L7	117	713/182,183,185,202.ccls. and (pass password passcode) and (cellular cellphone) and account	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/07/19 09:40
L8	41	713/185.ccls. and 713/202.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/07/19 09:48
L9	2	379/114.2.ccls. and ("709"/$.ccls. "713"/$.ccls.)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/07/19 09:49
L10	185	379/114.2.ccls. and network	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/07/19 10:04
L11	42	379/114.2.ccls. and network and (password passcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/07/19 09:52
L12	45	"5265155"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/07/19 10:06
L13	0	"5265155" and (passsword passcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/07/19 10:04

L14	76	"5265155" "5440621"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/07/19 10:14
L15	15	("5265155" "5440621") and (password passcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/07/19 10:06
L16	82	"5265155" "5440621" "5774535"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/07/19 11:15
L17	1	"6012088".PN.	USPAT; USOCR	OR	ON	2005/07/19 11:00
L18	1	"6003770".PN.	USPAT; USOCR	OR	ON	2005/07/19 11:11
L19	1	"5953398".PN.	USPAT; USOCR	OR	ON	2005/07/19 11:11
L20	1	"5909549".PN.	USPAT; USOCR	OR	ON	2005/07/19 11:12
L21	1	"5802502".PN.	USPAT; USOCR	OR	ON	2005/07/19 11:12
L22	1	"5793763".PN.	USPAT; USOCR	OR	ON	2005/07/19 11:12
L23	1	"5749075".PN.	USPAT; USOCR	OR	ON	2005/07/19 11:13
L24	47	"5749075"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/07/19 11:43
L26	8	709/219.ccls. and cellphone and (password passcode)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/19 14:31
S970	34	cellular and (temporary adj account)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/18 09:49
S971	62	cellular and ((temporary guest) adj account)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/18 09:53

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571) 273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

20995 7590 08/08/2005

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

OIPE IAP11 NOV 07 2005 PATENT & TRADEMARK OFFICE

11/07/2005 GWORDOF2 00000063 09519829

01 FC:2501 700.00 OP
02 FC:8001 30.00 OP

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Aaron D. Barker	(Depositor's name)
Aaron D. Barker	(Signature)
November 4, 2005	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/519,829	03/06/2000	Sten-Olov Engberg	APRILS.001A	8563

TITLE OF INVENTION: USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$700	$0	$700	11/08/2005

EXAMINER	ART UNIT	CLASS-SUBCLASS
HENEGHAN, MATTHEW E	2134	713-185000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Knobbe, Martens,
2 Olson & Bear LLP
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: April System Design AB
(B) RESIDENCE: (CITY and STATE OR COUNTRY): Solna, Sweden

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are enclosed:
☒ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☒ Advance Order - # of Copies 10

4b. Payment of Fee(s):
☒ A check in the amount of the fee(s) is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized by charge the ~~required~~ deficient fee(s), or credit any overpayment, to Deposit Account Number 11-1410 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

The Director of the USPTO is requested to apply the Issue Fee and Publication Fee (if any) or to re-apply any previously paid issue fee to the application identified above.
NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature Aaron D. Barker Date November 4, 2005

Typed or printed name Aaron D. Barker Registration No. 51,432

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

IPE IAP11
NOV 07 2005
PATENT & TRADEMARK OFFICE

PATENT

Case Docket No. APRILS.001A
Date: November 4, 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s)	:	Sten-Olov Engberg, et al.
Appl. No.	:	09/519,829
Filed	:	March 6, 2000
For	:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
Group Art Unit	:	2134
Class/Sub-Class	:	713-185000
Examiner	:	M. Heneghan

I hereby certify that this correspondence and all marked attachments are being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Issue Fee, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on

November 4, 2005
(Date)
Aaron D. Barker
Aaron D. Barker, Reg. No. 51,432

TRANSMITTAL LETTER

MAIL STOP ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Enclosed for filing is the Issue Fee for the above-identified application:

(X) Form PTOL-85.

(X) A check in the amount of $730 to cover the issue fee and advanced order of copies is enclosed.

(X) The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment, to Account No. 11-1410.

(X) Return prepaid postcard.

Aaron D. Barker
Registration No. 51,432
Attorney of Record
Customer No. 20,995
(949) 760-0404

2047934:ctc//110405

Knobbe Martens Olson & Bear LLP
Intellectual Property Law

2040 Main Street
Fourteenth Floor
Irvine, CA 92614
Tel 949-760-0404
Fax 949-760-9502
www.kmob.com

Stephen C. Jensen
sjensen@kmob.com

February 20, 2007

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Re: Title: **USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION**
Letters Patent No. 6,993,658
Issued: January 31, 2006
Our Reference: APRILS.001A

Dear Sir:

Enclosed for filing is a Certificate of Correction in connection with the above-identified patent.

As the errors cited in the Certificate of Correction were incurred through the fault of the Applicant, enclosed is our check in the amount of $100. Please charge any additional fees to our Deposit Account No. 11-1410.

Respectfully submitted,

Knobbe, Martens, Olson & Bear, LLP

Stephen C. Jensen
Registration No. 35,556
Customer No. 20,995

Enclosures

2571927
050206

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 6.003.659 B1
APPLICATION NO. : 09/519,829
ISSUE DATE : January 31, 2006
INVENTOR(S) : Engberg, et al.

It is certified that errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Sheet 1 of 1 List of References cited by applicant and considered by examiner, Entry 1, line 1 (Other Documents), Page 2, Column 1 (Other Publications), delete "computerterps" and insert -- computerps --.

Sheet 1 of List of References cited by applicant and considered by examiner, Entry 1, line 1 (Other Documents), Page 2, Column 1 (Other Publications), delete "html," and insert -- html.--

Sheet 1 of List of References cited by applicant and considered by examiner, Entry 3, line 1 (Other Documents), Page 2, Column 2 (Other Publications), delete "Authenication" and insert – Authentication --.

2571539
050206

MAILING ADDRESS OF SENDER:

Stephen C. Jensen
KNOBBE, MARTENS, OLSON & BEAR, LLP
2040 Main Street, 14th Floor
Irvine, California 92614

DOCKET NO. APRILS.001A

PTOSB/44 Equivalent

Electronic Patent Application Fee Transmittal

Application Number:	09519829
Filing Date:	06-Mar-2000
Title of Invention:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
First Named Inventor/Applicant Name:	Sten-Olov Engberg
Filer:	Stephen C. Jensen/Dolorna Ward
Attorney Docket Number:	APRILS.001A

Filed as Small Entity

Utility Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Certificate of correction	1811	1	100	100
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**100**

Electronic Acknowledgement Receipt	
EFS ID:	1528306
Application Number:	09519829
International Application Number:	
Confirmation Number:	8563
Title of Invention:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
First Named Inventor/Applicant Name:	Sten-Olov Engberg
Customer Number:	20995
Filer:	Stephen C. Jensen/Kehinde Jegede
Filer Authorized By:	Stephen C. Jensen
Attorney Docket Number:	APRILS.001A
Receipt Date:	20-FEB-2007
Filing Date:	06-MAR-2000
Time Stamp:	15:07:42
Application Type:	Utility

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	$100
RAM confirmation Number	122
Deposit Account	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)

1	Request for Certificate of Correction	Cert_of_Correction.pdf	70750	no	2
Warnings:					
Information:					
2	Fee Worksheet (PTO-06)	fee-info.pdf	8177	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	78927		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 6,993,658 B1
APPLICATION NO. : 09/519829
DATED : January 31, 2006
INVENTOR(S) : Engberg et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On Title Page

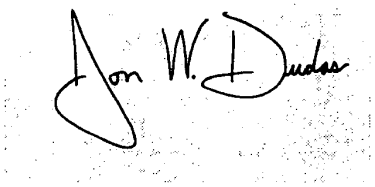
Item 56 Sheet 1 of 1 List of References cited by applicant and considered by examiner, Entry 1, line 1 (Other Documents), Page 2, Column 1 (Other Publications), delete "computerterps" and insert -- computerps --.

Item 56 Sheet 1 of List of References cited by applicant and considered by examiner, Entry 1, line 1 (Other Documents), Page 2, Column 1 (Other Publications), delete "html," and insert -- html.--

Item 56 Sheet 1 of List of References cited by applicant and considered by examiner, Entry 3, line 1 (Other Documents), Page 2, Column 2 (Other Publications), delete "Authenication" and insert -- Authentication --.

Signed and Sealed this

Third Day of April, 2007



JON W. DUDAS
Director of the United States Patent and Trademark Office

PTO/SB/123 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

CHANGE OF CORRESPONDENCE ADDRESS
Patent

Address to:
Mail Stop Post Issue
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Patent Number	6993658
Issue Date	01/31/2006
Application Number	09/519829
Filing Date	03/06/2000
First Named Inventor	Sten-Olov Engberg
Attorney Docket Number	APRILS.001A

Please change the Correspondence Address for the above-identified patent to:

☐ The address associated with Customer Number: [ ]

OR

☑ **Firm *or* Individual Name** Bjorn Karlsson, April System Design AB

Vretenvagen 10, III

Address

City Solna	**State**	**ZIP** 171 54
Country Sweden		
Telephone 011 46 8 5090 6100	**Email**	

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

This form will not affect any "fee address" provided for the above-identified patent. To change a "fee address" use the "Fee Address Indication Form" (PTO/SB/47).

I am the:

☐ Patentee.

☐ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

☑ Attorney or agent of record. Registration Number 35556.

Signature

Typed or Printed Name Stephen C. Jensen

Date June 19, 2012	Telephone 949-760-0404

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop Post Issue, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt	
EFS ID:	13054051
Application Number:	09519829
International Application Number:	
Confirmation Number:	8563
Title of Invention:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
First Named Inventor/Applicant Name:	Sten-Olov Engberg
Customer Number:	20995
Filer:	John M. Grover/Nino Lopez
Filer Authorized By:	John M. Grover
Attorney Docket Number:	APRILS.001A
Receipt Date:	19-JUN-2012
Filing Date:	06-MAR-2000
Time Stamp:	18:21:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Change of Address	20120619140238.pdf	130230 ac5d66ce59b0d1121cd1ada7cf59bfd21b9e9021	no	2
Warnings:					
Information:					

Total Files Size (in bytes):	130230

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

CANCELLED

OPAP AUG 20 2014 IAP11 PATENT & TRADEMARK OFFICE

OPAP AUG 20 2012 IAP11 PATENT & TRADEMARK OFFICE

1 fw

PTO/SB/123 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

CHANGE OF CORRESPONDENCE ADDRESS
Patent

Address to:
Mail Stop Post Issue
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Patent Number	6993658
Issue Date	01/31/2006
Application Number	09/519829
Filing Date	03/06/2000
First Named Inventor	Sten-Olov Engberg
Attorney Docket Number	APRILS.001A

Please change the Correspondence Address for the above-identified patent to:

☐ The address associated with Customer Number: [ ]

OR

☑ **Firm *or* Individual Name** Bjorn Karlsson, April System Design AB

Vretenvagen 10, III

Address

City Solna **State** **ZIP** 171 54

Country Sweden

Telephone 011 46 8 5090 6100 **Email**

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

This form will not affect any "fee address" provided for the above-identified patent. To change a "fee address" use the "Fee Address Indication Form" (PTO/SB/47).

I am the:

☐ Patentee.

☐ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

☑ Attorney or agent of record. Registration Number 35556.

Signature

Typed or Printed Name Stephen C. Jensen

Date June 19, 2012 Telephone 949-760-0404

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop Post Issue, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov





CUSTOMER NUMBER: 000107538

CORRESPONDENCE ADDRESS:

Bjorn Karlsson . April System Design AB
Vretenvagen 10, III
Solna, 71754
SWEDEN

FAX: 1146850906130 **PHONE:** 114685090610

E-MAIL:

Date Mailed: 06/25/2012

NOTICE OF CUSTOMER NUMBER ASSIGNMENT

The request to assign a "Customer Number" to the above-identified Correspondence Address and Practitioner Registration Number(s) indicated below has been accepted by the Office.

The Customer Number as assigned above may be used to identify the correspondence address or "fee address" for, and/or the appointed practitioner(s) in, a United States patent application or patent. Any existing PKI certificates of the practitioners listed below are associated with the above-identified Customer Number.

PRACTITIONER REGISTRATION NUMBER(S) ASSIGNED TO THAT CUSTOMER NUMBER:

Patents Electronic Business Center
866-217-9197 (toll-free) or 571-272-4100

PART 1 - ATTORNEY/APPLICANT COPY





To: USPTO

Mail Stop Post Issue
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
USA

Stockholm 2012-08-14

It seems like you have the wrong zip code for our company address in your files. The "fee address" was recently changed by our Attorney. Since the address change, we have received a couple of letters, both with the same, but wrong, zip code. This may cause mail delay and we would like you to change it.

Attached is a copy of the original "CHANGE OF CORRESPONDANCE ADDRESS" form. Attached are also a couple of copies of mail from you with the wrong zip code.

Our zip code should be **171 54**.

Best Regards,

Björn Karlsson, CEO

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
Stylesheet Version v1.2

EPAS ID: PAT2737239

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	CHANGE OF ADDRESS

CONVEYING PARTY DATA

Name	Execution Date
DYNAPASS, INC.	02/21/2014

RECEIVING PARTY DATA

Name:	DYNAPASS, INC.
Street Address:	555 ANTON BLVD.
Internal Address:	SUITE 850
City:	COSTA MESA
State/Country:	CALIFORNIA
Postal Code:	92626

PROPERTY NUMBERS Total: 1

Property Type	Number
Patent Number:	6993658

CORRESPONDENCE DATA

Fax Number: (888)389-3542
Phone: 9099642272
Email: miguel.medina@dynapass.com
Correspondence will be sent via US Mail when the email attempt is unsuccessful.
Correspondent Name: MIGUEL MEDINA
Address Line 1: 555 ANTON BLVD.
Address Line 2: SUITE 850
Address Line 4: COSTA MESA, CALIFORNIA 92626

NAME OF SUBMITTER:	MIGUEL MEDINA
Signature:	/miguel medina/
Date:	02/21/2014
	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 1
source=DynaPass Patent Change of Address#page1.tif

Documentation not required for Patent change of address:

Previous Address:

DynaPass, Inc.
575 Anton Blvd. Suite 1150
Costa Mesa, CA 92626

New Address:

DynaPass, Inc.
555 Anton Blvd. Suite 850
Costa Mesa, CA 92626

RECEIVED
CENTRAL FAX CENTER
SEP 18 2017

PTO/SB/47 (03-09)
Approved for use through 07/31/2012. OMB 0651-0015
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

"FEE ADDRESS" INDICATION FORM

Address to:
Mail Stop M Correspondence
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

- OR -

Fax to:
571-273-6500

INSTRUCTIONS: The issue fee must have been paid for application(s) listed on this form. In addition, only an address represented by a Customer Number can be established as the fee address for maintenance fee purposes (hereafter, fee address). A fee address should be established when correspondence related to maintenance fees should be mailed to a different address than the correspondence address for the application. **When to check the first box below:** If you have a Customer Number to represent the fee address. **When to check the second box below:** If you have no Customer Number representing the desired fee address, in which case a completed Request for Customer Number (PTO/SB/125) must be attached to this form. For more information on Customer Numbers, see the Manual of Patent Examining Procedure (MPEP) § 403.

For the following listed application(s), please recognize as the "Fee Address" under the provisions of 37 CFR 1.363 the address associated with:

☐ Customer Number: 151075

OR

☒ The attached Request for Customer Number (PTO/SB/125) form.

PATENT NUMBER (if known)	APPLICATION NUMBER
6993658	09519829

Completed by (check one):

☐ Applicant/Inventor

☐ Attorney or Agent of record _ (Reg. No.)

☒ Assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☐ Assignee recorded at Reel Frame_

Signature

Fredrik Bohman, DynaPass Inc
Typed or printed name

855-396-2727
Requester's telephone number

9/15/17
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ * Total of forms are submitted.

This collection of information is required by 37 CFR 1.363. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 5 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND COMPLETED FORMS TO THIS ADDRESS.
SEND TO: Mail Stop M Correspondence, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

OPAP AKIMA-14 SEP 15 2017 PATENT & TRADEMARK OFFICE

PTO/SB/123 (04-15)
Approved for use through 01/31/2018. OMB 0651-0035
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

CHANGE OF CORRESPONDENCE ADDRESS
Patent

Address to:
Mail Stop Post Issue
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Patent Number	6993658
Issue Date	01/31/2006
Application Number	09519829
Filing Date	03/06/2000
First Named Inventor	Sten-Olov Engberg
Attorney Docket Number	APRILS.001A

Please change the Correspondence Address for the above-identified patent to:

☒ The address associated with Customer Number: 151075

OR

☐ **Firm *or* Individual Name**

Address

City | **State** | **ZIP**

Country

Telephone | **Email**

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

This form will not affect any "fee address" provided for the above-identified patent. To change a "fee address" use the "Fee Address Indication Form" (PTO/SB/47).

I am the:

☐ Patentee.

☒ Assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

☐ Attorney or agent of record. Registration Number _____.

Signature Fredrik Bohman

Typed or Printed Name Fredrik Bohman, DynaPass Inc

Date 09/15/2017 Telephone 855-396-2727

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office. U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop Post Issue, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

RECEIVED OPAP SEP 20 2017

PETITION TO ACCEPT UNINTENTIONALLY DELAYED PAYMENT OF MAINTENANCE FEE IN AN EXPIRED PATENT (37 CFR 1.378(b))

Patent Number	Issue Date	Application Number	Filing Date	Docket Number (if applicable)
6993658	31-Jan-2006	09519829	06-Mar-2000	

CAUTION: Maintenance fee (and surcharge, if any) payment must correctly identify: (1) the patent number and (2) the application number of the actual U.S. application leading to issuance of that patent to ensure the fee(s) is/are associated with the correct patent. 37 CFR 1.366(c) and (d).

Applicants claims the following fee status:

- (◉) Small Entity
- ( ) Micro Entity
- ( ) Regular Undiscounted

Applicants selects the following :

( ) 3 1/2	( ) 7 1/2	(◉) 11 1/2

PETITION FEE
The petition fee required by 37 CFR 1.17(m) (Fee Code 1558/2558) must be paid as a condition of accepting unintentionally delayed payment of the maintenance fee.

MAINTENANCE FEE (37 CFR 1.20(e)-(g))
The appropriate maintenance fee must be submitted with this petition.

STATEMENT
THE UNDERSIGNED CERTIFIES THAT THE DELAY IN PAYMENT OF THE MAINTENANCE FEE TO THIS PATENT WAS UNINTENTIONAL

PETITIONER(S) REQUEST THAT THE DELAYED PAYMENT OF THE MAINTENANCE FEE BE ACCEPTED AND THE PATENT REINSTATED

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

37 CFR 1.378(c) states: "Any petition under this section must be signed in compliance with 37 CFR 1.33(b) ."

I certify, in accordance with 37 CFR 1.4(d)(4) that I am

- ( ) An attorney or agent registered to practice before the Patent and Trademark Office who has been given power of attorney in this application.
- ( ) An attorney or agent registered to practice before the Patent and Trademark Office
- ( ) A sole patentee
- ( ) A joint patentee; I certify that I am authorized to sign this submission on behalf of all the other patentees as evidenced by the power of attorney in the application
- ( ) A joint patentee; all of whom are signing this e-petition
- (◉) The assignee of record of the entire interest that qualifies as an authorized party under 37 CFR 1.33(b)

The Assignee of record of the entire interest			
Under 37 CFR 3.71 an assignee becomes of record by filing a statement in compliance with 37 CFR 3.73(b). Signature requirements are set forth in 37 CFR 1.4(d), and the undersigned certifies that he / she is empowered to act on behalf of the assignee of the entire interest			
Signature	/Fredrik Bohman/		
Name	Fredrik Bohman		
Enter Reel and Frame Number			Remove
Reel Number		Frame Number	
Click ADD for additional Reel Number and Frame Number			Add

Electronic Patent Application Fee Transmittal

Application Number:	09519829
Filing Date:	06-Mar-2000
Title of Invention:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
First Named Inventor/Applicant Name:	Sten-Olov Engberg
Filer:	Fredrik Bohman
Attorney Docket Number:	APRILS.001A

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
MAINTENANCE FEE DUE AT 11.5 YEARS	2553	1	3700	3700
PET. DELAY PYMT MAINTAIN PATENT IN FORCE	2558	1	1000	1000
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	4700

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

In re Patent No. 6993658
Issue Date: January 31,2006
Application No. 09519829
Filed: March 6,2000
Attorney Docket No. APRILS.001A

:
:DECISION GRANTING PETITION
:UNDER 37 CFR 1.378(b)
:

This is a decision on the electronic petition, filed February 6,2018 ,under 37 CFR 1.378(b) to accept the unintentionally delayed payment of the 11.5 year maintenance fee for the above-identified patent.

The petition is **GRANTED**.

The maintenance fee is accepted, and the above-identified patent reinstated as of February 6,2018 . This decision also constitutes notice that the fee has been accepted. An electronic copy of the petition and this decision has been created as an entry in the Image File Wrapper. Nevertheless, petitioner should print and retain an independent copy.

Telephone inquiries related to this electronic decision should be directed to the Electronic Business Center at 1-866-217-9197.

Electronic Acknowledgement Receipt	
EFS ID:	31715942
Application Number:	09519829
Patent Number:	6993658
Confirmation Number:	8563
Petition Issued Date:	February 6,2018
Title of Invention:	USE OF PERSONAL COMMUNICATION DEVICES FOR USER AUTHENTICATION
First Named Inventor/Applicant Name:	Sten-Olov Engberg
Customer Number:	151075
Filer:	Fredrik Bohman
Filer Authorized By:	
Attorney Docket Number:	APRILS.001A
Receipt Date:	06-FEB-2018
Filing Date:	06-MAR-2000
Time Stamp:	15:32:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$4700
RAM confirmation Number	020718INTEFSW15341100
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Petition automatically granted by EFS	petition-request.pdf	33774 8d8544404ee5cb913e4a7a949dbaf8469e573ec6	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	31931 1e51dee6018cadadea69ee42cd4cfdecc644816e	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	65705		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
Stylesheet Version v1.2

EPAS ID: PAT7100640

SUBMISSION TYPE:	NEW ASSIGNMENT
NATURE OF CONVEYANCE:	ASSIGNMENT

CONVEYING PARTY DATA

Name	Execution Date
DYNAPASS, INC.	11/12/2021

RECEIVING PARTY DATA

Name:	DYNAPASS IP HOLDINGS LLC
Street Address:	16192 COASTAL HIGHWAY
City:	LEWES
State/Country:	DELAWARE
Postal Code:	19958

PROPERTY NUMBERS Total: 1

Property Type	Number
Patent Number:	6993658

CORRESPONDENCE DATA

Fax Number: (302)645-1280

Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.

Phone: 9099642272
Email: miguel.medina@dynapass.com
Correspondent Name: DYNAPASS, INC.
Address Line 1: 16192 COASTAL HIGHWAY
Address Line 4: LEWES, DELAWARE 19958

NAME OF SUBMITTER:	MIGUEL MEDINA
SIGNATURE:	/MM/
DATE SIGNED:	01/02/2022
	This document serves as an Oath/Declaration (37 CFR 1.63).

Total Attachments: 3
source=DynaPass '658 Patent Asignment Agreement with Dynapass IP Holdings LLC-11-12-21 (1)#page1.tif
source=DynaPass '658 Patent Asignment Agreement with Dynapass IP Holdings LLC-11-12-21 (1)#page2.tif
source=DynaPass '658 Patent Asignment Agreement with Dynapass IP Holdings LLC-11-12-21 (1)#page3.tif

ASSIGNMENT OF U.S PATENT NO. 6,993,658

DynaPass, Inc., a Delaware Corporation organized under and pursuant to the laws of the State of Delaware (hereinafter referred to as "Assignor"), is the sole and exclusive owner of the U.S. Patent No. 6,993,658 listed in Exhibit A (hereinafter referred to as " '658 Patent); and

Dynapass IP Holdings, a Limited Liability Company and a wholly owned subsidiary of DynaPass, Inc. organized under and pursuant to the laws of the State of Delaware (hereinafter referred to as "Assignee"), desires to acquire the right, title and interest in, to and under said '658 Patent and the inventions covered thereby.

For good and valuable consideration, the receipt and sufficiency of which Assignor acknowledges, Assignor hereby sells, assigns, transfers, and sets over to Assignee, its successors, legal representatives and assigns, the entire right, title and interest in and to said '658 Patent and all improvements thereon, and all provisional, original, divisional, continuation, continuation in part, substitute or reissue applications and patents applied for or granted therefor (including related rights such as utility model registrations, inventor's certificates and the like), in the United States of America and all other countries, which claim priority to the Patent Matters including, without limitation , all United States Letters Patents and all reissues, reexaminations and extensions thereof and all priority rights under all available international agreements, treaties and conventions for the protection of intellectual property in its various forms in every participating country, and the Commissioner of Patents and Trademarks is hereby authorized and requested to issue all patents resulting from the '658 Patent to said Assignee herein, as assignee of the entire interest therein; and the Assignor for itself and its legal representatives, heirs and assigns does hereby agree and covenant without further remuneration, to execute and deliver all original, divisional, continuation, continuation in part, reissue and other applications for Letters Patent and all assignments thereof to said Assignee or its successors, legal representatives and assigns, to communicate to said Assignee or its successors, legal representatives and assigns all facts known to the Assignor respecting said '658 Patent whenever requested, to testify in any interferences or other legal proceedings in which said applications or patents may become involved, to sign all lawful papers, make all rightful oaths, and do generally everything necessary to aid Assignee, its successors, legal representatives and assigns to obtain patent protection for said '658 Patent in the United States of America and all other countries, the reasonable expenses incident to said '658 Patent to be borne and paid by said Assignee.

Assignor further assigns, transfers and conveys to Assignee all causes of action (whether known or unknown or whether currently pending, filed, or otherwise) and other enforcement rights under, or on account of, any of the '658 Patent including, without limitation, all causes of action and other enforcement rights for (l) damages, (2) injunctive relief, and (3) any other remedies of any kind for past, current, and future infringement.

The right, title, and interest conveyed in this Assignment is to be held and enjoyed by Assignee and Assignee's successors as fully and exclusively as it would have been held and enjoyed by Assignor had this assignment not been made. .

For and on behalf of

ASSIGNOR:

DynaPass, Inc.

By: _____

Name: **Steve Carter**

Title: **COO and Board Member, DynaPass, Inc.**

Date: NOV. 12, 2021

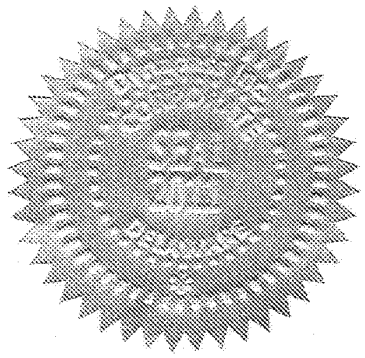


EXHIBIT A

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

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00210	6/17/2022	Eastern District of Texas

PLAINTIFF	DEFENDANT
DYNAPASS IP HOLDINGS LLC	BANK OF AMERICA CORPORATION AND BANK OF AMERICA, N.A.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,993,658	1/31/2006	DYNAPASS IP HOLDINGS LLC
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00213	6/17/2022	Eastern District of Texas

PLAINTIFF	DEFENDANT
DYNAPASS IP HOLDINGS LLC	PLAINSCAPITAL BANK AND HILLTOP HOLDINGS INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,993,658	1/31/2006	DYNAPASS IP HOLDINGS LLC
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00215	6/17/2022	Eastern District of Texas

PLAINTIFF	DEFENDANT
DYNAPASS IP HOLDINGS LLC	REGIONS FINANCIAL CORPORATION AND REGIONS BANK

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,993,658	1/31/2006	DYNAPASS IP HOLDINGS LLC
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00216	6/17/2022	Eastern District of Texas

PLAINTIFF	DEFENDANT
DYNAPASS IP HOLDINGS LLC	TRUIST FINANCIAL CORPORATION AND TRUIST BANK

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,993,658	1/31/2006	DYNAPASS IP HOLDINGS LLC
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:21-cv-00211	6/17/2022	Eastern District of Texas

PLAINTIFF	DEFENDANT
DYNAPASS IP HOLDINGS LLC	BOKF, NATIONAL ASSOCIATION

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,993,658	1/31/2006	DYNAPASS IP HOLDINGS LLC
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00212	6/17/2022	Eastern District of Texas

PLAINTIFF	DEFENDANT
DYNAPASS IP HOLDINGS LLC	JPMORGAN CHASE & CO., JPMORGAN CHASE BANK, NATIONAL ASSOCIATION AND CHASE BANK USA NATIONAL ASSOCIATION

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,993,658	1/31/2006	DYNAPASS IP HOLDINGS LLC
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00214	6/17/2022	Eastern District of Texas

PLAINTIFF	DEFENDANT
DYNAPASS IP HOLDINGS LLC	PNC FINANCIAL SERVICES GROUP, INC., PNC BANK, N.A., BBVA USA BANCHARES, INC., AND BBVA USA

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,993,658	1/31/2006	DYNAPASS IP HOLDINGS LLC
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00217	6/17/2022	Eastern District of Texas

PLAINTIFF	DEFENDANT
DYNAPASS IP HOLDINGS LLC	WELLS FARGO & COMPANY AND WELLS FARGO BANK, N.A.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,993,658	1/31/2006	DYNAPASS IP HOLDINGS LLC
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00218	6/17/2022	Eastern District of Texas

PLAINTIFF	DEFENDANT
DYNAPASS IP HOLDINGS LLC	WOODFOREST NATIONAL BANK AND WOODFOREST FINANCIAL GROUP, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	6,993,658	1/31/2006	DYNAPASS IP HOLDINGS LLC
2			
3			
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

The United States Patent and Trademark Office
PATENT TRIAL AND APPEAL BOARD

A petition has been filed in Patent Number 6,993,658, Application Number 09/519,829 on January 6, 2023.

The Case Number is IPR2023-00425.

To view the documents filed in this petition, go to https://ptab.uspto.gov.

Use the Search PTAB tab and enter the Patent Number or the Trial or Case Number and select the Search button.

Questions regarding this notice should be directed to the Patent Trial and Appeal Board at 571-272-7822.

Trials@uspto.gov
571-272-7822

Paper No. 5

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, LLC
Petitioner,

v.

DYNAPASS IP HOLDINGS LLC
Patent Owner.

IPR2023-00425
Patent 6,993,658

Mailed: January 25, 2023

Before Paula Conn, *Trial Paralegal*

NOTICE OF FILING DATE ACCORDED TO PETITION
AND
TIME FOR FILING PATENT OWNER PRELIMINARY RESPONSE

The petition for *inter partes* review, filed in the above proceeding has been accorded the filing date of January 6, 2023.

Patent Owner may file a preliminary response to the petition no later than three months from the date of this notice. The preliminary response is limited to setting forth the reasons why the requested review should not be instituted. Patent Owner may also file an election to waive the preliminary response to expedite the proceeding. For more information, please consult

the Office Patent Trial Practice Guide, 77 Fed. Reg. 48756 (Aug. 14, 2012), which is available on the Board Web site at http://www.uspto.gov/PTAB.

Patent Owner is advised of the requirement to submit mandatory notice information under 37 C.F.R. § 42.8(a)(2) within 21 days of service of the petition.

The parties are encouraged to use the heading on the first page of this Notice for all future filings in the proceeding.

The parties are advised that under 37 C.F.R. § 42.10(c), recognition of counsel pro hac vice requires a showing of good cause. The parties are authorized to file motions for pro hac vice admission under 37 C.F.R. § 42.10(c). Such motions shall be filed in accordance with the "Order -- Authorizing Motion for Pro Hac Vice Admission" in Case IPR2013-00639, Paper 7, a copy of which is available on the Board Web site under "Representative Orders, Decisions, and Notices." **The parties are reminded that, in order for any motion for *pro hac vice* admission to be considered by the Board, the requisite fees must first be paid.** The current fee schedule is available at https://www.uspto.gov/learning-and-resources/fees-and-payment/uspto-fee-schedule.

The parties are reminded that unless otherwise permitted by 37 C.F.R. § 42.6(b)(2), all filings in this proceeding must be made electronically in Patent Trial and Appeal Board End to End (PTAB E2E), accessible from the Board Web site at http://www.uspto.gov/PTAB. To file documents, users must register with PTAB E2E. Information regarding how to register with and use PTAB E2E is available at the Board Web site.

If there are any questions pertaining to this notice, please contact Paula Conn at 571-272-4589 or the Patent Trial and Appeal Board at 571-272-7822.

PETITIONER:

Jordan Rossen
Ashraf Fawzy
UNIFIED PATENTS LLC
jordan@unifiedpatents.com
afawzy@unifiedpatents.com

PATENT OWNER:

John Wittenzellner
Todd Landis
Michael Fagan
WILLIAMS SIMONS & LANDIS PLLC
johnw@wsltrial.com
tlandis@wsltrial.com
mfagan@wsltrial.com

NOTICE CONCERNING ALTERNATIVE DISPUTE RESOLUTION (ADR)

The Patent Trial and Appeal Board (PTAB) strongly encourages parties who are considering settlement to consider alternative dispute resolution as a means of settling the issues that may be raised in an AIA trial proceeding. Many AIA trials are settled prior to a Final Written Decision. Those considering settlement may wish to consider alternative dispute resolution techniques early in a proceeding to produce a quicker, mutually agreeable resolution of a dispute or to at least narrow the scope of matters in dispute. Alternative dispute resolution has the potential to save parties time and money.

Many non-profit organizations, both inside and outside the intellectual property field, offer alternative dispute resolution services. Listed below are the names and addresses of several such organizations. The listings are provided for the convenience of parties involved in cases before the PTAB; the PTAB does not sponsor or endorse any particular organization's alternative dispute resolution services. In addition, consideration may be given to utilizing independent alternative dispute resolution firms. Such firms may be located through a standard keyword Internet search.

CPR INSTITUTE FOR DISPUTE RESOLUTION	AMERICAN INTELLECTUAL PROPERTY LAW ASSOCIATION (AIPLA)	AMERICAN ARBITRATION ASSOCIATION (AAA)	WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO)	AMERICAN BAR ASSOCIATION (ABA)
Telephone: (212) 949-6490	Telephone: (703) 415-0780	Telephone: (212) 484-3266	Telephone: 41 22 338 9111	Telephone : (202) 662-1000
Fax: (212) 949-8859	Fax: (703) 415-0786	Fax: (212) 307-4387	Fax: 41 22 733 5428	N/A
575 Lexington Ave	241 18th Street, South, Suite 700	140 West 51st Street	34, chemin des Colombettes	1050 Connecticut Ave, NW
New York, NY 10022	Arlington, VA 22202	New York, NY 10020	CH-1211 Geneva 20, Switzerland	Washington D.C. 20036
www.cpradr.org	www.aipla.org	www.adr.org	www.wipo.int	www.americanbar.org

If parties to an AIA trial proceeding consider using alternative dispute resolution, the PTAB would like to know whether the parties ultimately decided to engage in alternative dispute resolution and the reasons why or why not. If the parties actually engage in alternative dispute resolution, the

PTAB would be interested to learn what mechanism (e.g., arbitration, mediation, etc.) was used and the general result. Such a statement from the parties is not required but would be helpful to the PTAB in assessing the value of alternative dispute resolution to parties involved in AIA trial proceedings. To report an experience with ADR, please forward a summary of the particulars to the following email address: PTAB_ADR_Comments@uspto.gov

Patent Trial and Appeal Board

A petition has been filed in Patent Number 6,993,658, Application Number 09/519,829, on January 3, 2023.

The AIA Review Number is IPR2023-00367.

To view the documents filed in this petition, go to https://ptab.uspto.gov and Search for the AIA Review Number.

- Enter your search criteria on the "Search PTAB" page
- Type in the AIA Review Number or Patent Number
- You will need to answer the CAPTCHA to prove that you are not a robot.
- Click on the "Search" button
- The search results will appear identifying the AIA Review Number
- Click on the "View Documents" button
- A pop-up window will appear with a list of documents
- Click on the "Download" button to download the document.

Questions regarding this notice should be directed to the Patent Trial and Appeal Board at 571-272-7822.

Trials@uspto.gov
571-272-7822

Paper 13
Date: July 18, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

BANK OF AMERICA, N.A.; TRUIST BANK; BOKF, N.A.; WELLS FARGO BANK, N.A.; AND PNC BANK, N.A.,
Petitioner,

v.

DYNAPASS IP HOLDINGS LLC,
Patent Owner.

IPR2023-00367
Patent 6,993,658 B1

Before KEVIN F. TURNER, KRISTEN L. DROESCH, and LYNNE H. BROWNE, *Administrative Patent Judges.*

BROWNE, *Administrative Patent Judge.*

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Bank of America, Truist Bank, BOKF, Wells Fargo Bank, and PNC Bank (collectively "Petitioners") filed a Petition (Paper 1 ("Pet.")) requesting institution of an *inter partes* review of claims 1–3 and 5–7 of U.S. Patent No. 6,993,658 B1 (Ex. 1001, "the '658 Patent"). Pet. 1, 95–96; Papers 2–6 (Powers of Attorney). Dynapass IP Holdings LLC ("Patent Owner") timely filed a Preliminary Response. Paper 8 ("Prelim. Resp."). Prelim. Resp. 1. With our authorization, Petitioner filed a Preliminary Reply (Paper 11, "Reply") and Patent Owner filed a Preliminary Sur-reply (Paper 12, "Sur-reply").

Under 35 U.S.C. § 314(a), an *inter partes* review may not be instituted unless the information presented in the Petition and any response thereto shows "there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." Upon consideration of the Petition and the evidence of record, we conclude that the Petition fails to establish that there is a reasonable likelihood that Petitioner would prevail in challenging at least one of claims 1–3 and 5–7 of the '658 Patent as unpatentable under the grounds presented in the Petition. Pursuant to § 314, we deny institution of an *inter partes* review as to the challenged claims of the '658 Patent.

A. Real Parties in Interest

Petitioner identifies the real party-in-interest as Bank of America Corporation, Bank of America, N.A., BOKF, N.A., Okta, Inc., Truist Bank, Truist Financial Corp., Wells Fargo Bank, N.A., Wells Fargo & Company, PNC Bank, N.A., and The PNC Financial Services Group, Inc. Pet. 95–96.

Patent Owner identifies itself, Dynapass IP Holdings LLC and DynaPass Inc., as real parties-in-interest. Paper 7, 1.

B. Related Matters

The parties identify the following litigations as related district court matters: *Dynapass IP Holdings LLC v. Bank of America Corporation et al*, 2:22-cv-00210 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. BOKF, National Association et al*, 2:22-cv-00211 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. JPMorgan Chase & Co. et al*, 2:22-cv-00212 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. PlainsCapital Bank et al*, 2:22-cv-00213 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. PNC Financial Services et al*, 2:22-cv-00214 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Regions Financial Corporation et al*, 2:22-cv-00215 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Truist Financial Corporation et al*, 2:22-cv-00216 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Wells Fargo & Company et al*, 2:22-cv-00217 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Woodforest National Bank et al*, 2:22-cv-00218 (EDTX 6-17-2022). Pet. 96–97; Paper 7, 1–2.

Patent Owner also identifies *Unified Patents, LLC v. Dynapass IP Holdings LLC*, IPR2023-00425 as a related matter. Paper 7, 2.

C. The '658 Patent

The '658 Patent is titled "Use of Personal Communication Devices For User Authentication." Ex. 1001, code (54). The "invention relates to a system through which user tokens required for user authentication are supplied through personal communication devices such as mobile telephones and pagers." *Id.* at 1:8–11.

One embodiment of the invention provides a password setting system that includes a user token server and a communication module. The user token server generates a random token in response to a request for a new password from a user. Ex. 1001, 1:63–2:2. "The server creates a new password by concatenating a secret passcode that is known to the user with the token" and "sets the password associated with the user's user ID to be the new password." *Id.* at 2:2–6. The communication module transmits the token to a personal communication device, such as a mobile phone or a pager carried by the user." *Id.* at 2:6–8. Then, the user concatenates the secret passcode with the received token in order to form a valid password, which the user submits to gain access to the secure system. *Id.* at 2:8–11.

Figure 1, reproduced below, illustrates an overview, including system components, of a user authentication system 100 according to a preferred embodiment of the present invention." Ex. 1001, 4:2–4.

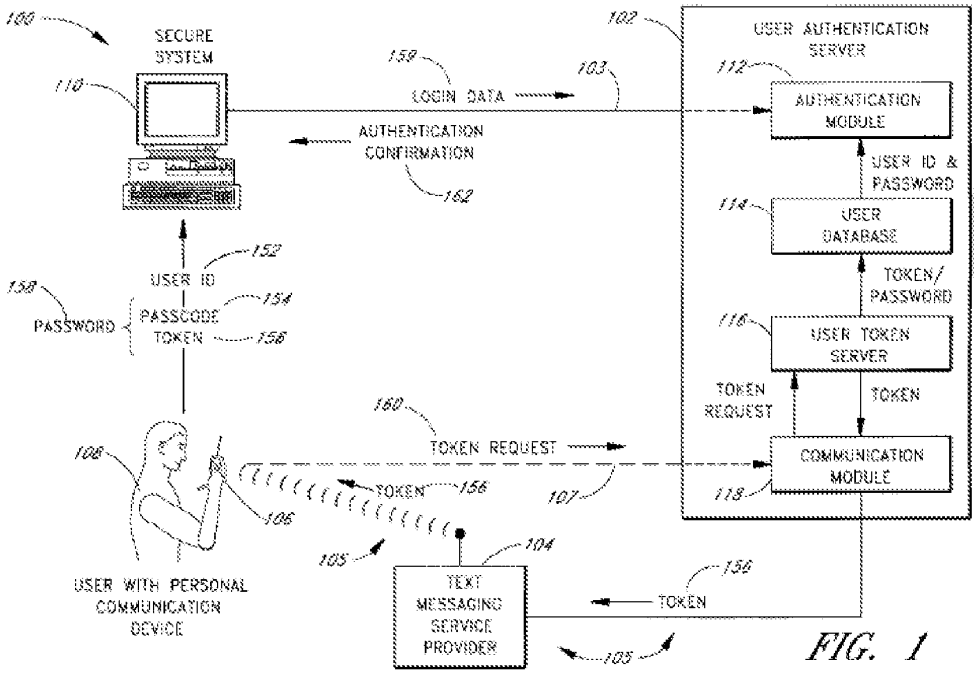


FIG. 1

User authentication system 100 includes authentication Server 102, text messaging Service provider 104, personal communication device 106 carried by user 108, and secure system 110 to which the authentication system 100 regulates access. *Id.* at 4:9–13. "[P]ersonal communication device 106 is preferably a pager or a mobile phone having SMS (short message Service) receive capability." *Id.* at 4:13–15. Secure system 110 can be "any system, device, account, or area to which it is desired to limit access to authenticated users." *Id.* at 4:18–20.

User authentication server 102 is configured to require that user 108 supply authentication information through secure system 110 in order to gain access to secure system 110. Ex. 1001, 4:32–35. Authentication information provided by the user includes user ID 152, passcode 154 and user token 156. *Id.* at 4:36–37. User ID 152 may be publicly known and

used to identify the user and passcode 154 is secret and only known to the user 108, whereas token 156 is provided only to user 108 by user authentication server 102 through personal communication device 106. *Id.* at 4:39–44. To gain access to secure system 100, user 108 combines token 156 with passcode 154 to form password 158. *Id.* at 4:52–53. Thus, user 108 needs to have personal communication device 106 in order to gain access to secure system 110. *Id.* at 4:46–48. Further, token 156 has a limited lifespan, such as 1 minute or 1 day. *Id.* at 4:44–45.

D. Illustrative Claims

Petitioner challenges claims 1–3 and 5–7. Claims 1 and 5, reproduced below with Petitioner's identifiers included, are the independent claims at issue in this proceeding. Ex. 1001, 11:43–12:13, 12:20–47. Dependent claims 2 and 3 depend from claim 1 and claim 6 and 7 depend from claim 5. *Id.* at 12:16–19, 12:48–52.

> 1. [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 computer 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.

5. [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 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, [5.d] the control module further configured to set a password associated with the user to be the new password;

[5.e] a communication module configured to transmit the token to the personal communication device through the cell phone network, and

[5.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, [5.g] 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.

Ex. 1001, 11:43–12:13, 12:20–47.

E. Prior Art and Asserted Grounds

Petitioner asserts that claims 1–3 and 5–7 would have been unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–3, 5–7	103	Guthrie,[1] Sormunen[2]
1–3, 5–7	103	Katou,[3,4] Guthrie

II. ANALYSIS

A. Level of Ordinary Skill in the Art

In determining the level of skill in the art, we consider the type of problems encountered in the art, the prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level of active workers in the field. *Custom Accessories v. Jeffrey-Allan Indus.*, 807 F.2d 955, 962 (Fed. Cir. 1986); *Orthopedic Equip. Co. v. U.S.*, 702 F.2d 1005, 1011 (Fed. Cir. 1983).

Petitioner contends that

> A person of ordinary skill in the art ("POSITA") would have at least a bachelor's degree in Electrical Engineering, Computer Science, Computer Engineering, or equivalent, and at

[1] US 6,161,185 to Guthrie et al., issued December 12, 2000 ("Guthrie") (Ex. 1007).
[2] WO 97/31306, published August 28, 1997 ("Sormunen") (Ex. 1008).
[3] In accordance with the English translation, the inventor is Katou, not Kato.
[4] JP 2000-10927 to Katou, published January 14, 2000 ("Katou") (Ex. 1005). For purposes of this Decision we rely on the English translation of Katou (Ex. 1006).

> least two years of prior experience with user authentication technologies for computer systems as of the earliest priority date of the '658 Patent—March 6, 2000. Additional education could substitute for professional experience and vice versa.

Pet. 3–4 (citing Ex. 1002 ¶ 23). "For the purposes of [the Preliminary] Response only, Patent Owner does not dispute the level of skill of a person of ordinary skill in the art ('POSITA') identified in the Petition." Prelim. Resp. 10.

Based on the record presented, including our review of the '658 patent and the types of problems and solutions described in the patent and the cited prior art, we adopt Petitioner's assessment of the level of ordinary skill in the art and apply it for purposes of this Decision.

B. Claim Construction

We apply the federal court claim construction standard that is used to construe a claim in a civil action under 35 U.S.C. § 282(b). This is the same claim construction standard articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc), and its progeny. Only terms that are in controversy need to be construed, and then only to the extent necessary to resolve the controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Matal*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (in the context of an *inter partes* review, applying *Vivid Techs. v. Am. Sci. & Eng'g*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

Petitioner contends that, "[f]or this IPR, the plain meaning of each claim term can be applied. Ex. 1002 ¶¶ 25–29." Patent Owner contends that "claim construction is not necessary for the Board to determine that the Petition fails to demonstrate a reasonable likelihood that any challenged claim of the '658 Patent is unpatentable." Prelim. Resp. 10.

At this stage of this proceeding, we agree with the parties that claim construction is not necessary to resolve the controversy.

C. Patentability Challenges

1. Principles of Law: Obviousness

A claim is unpatentable under 35 U.S.C. § 103 if "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." *KSR Int'l Co. v. Teleflex*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations.[5] *See Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17–18 (1966).

2. Relevant Prior Art

a) Guthrie (Ex. 1007)

Guthrie is a U.S. patent that issued December 12, 2000. Ex. 1107, code (45). Petitioner asserts that Guthrie is prior art under pre-AIA 35 U.S.C. § 102(e). Pet. 1.

[5] The current record does not present or address any evidence of nonobviousness.

Figure 5, reproduced below, shows Guthrie's system:

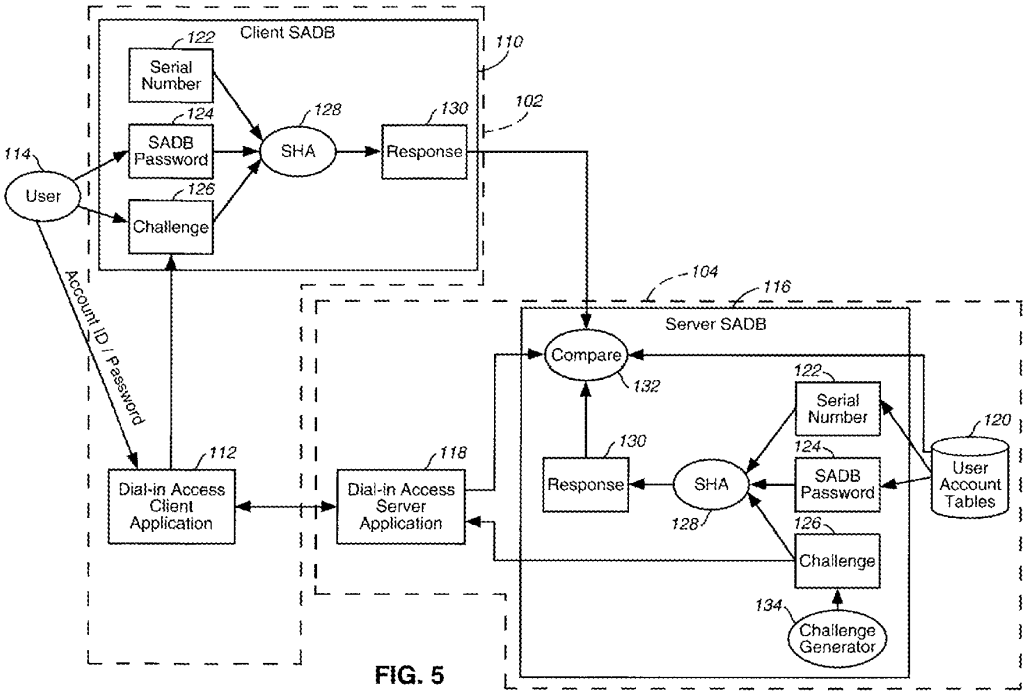


FIG. 5

Figure 5 is a block diagram showing Guthrie's personal authentication process. Ex. 1005, 3:25–26. As shown in Figure 5, user 114 initially inputs the user's account and correct password to client 102. *Id.* at 7:16–17. Client 102, via client application 112, transmits the user account and account password to the server 104. *Id.* at 7:17–19. Server 104 validates the user account and password against user 114's account table stored in user account database 120. *Id.* at 7:20–22. If initial validation is successful, then server 104 employs challenge generator 134 in its SADB[6] calculator 116 to generate challenge 126. *Id.* at 22–26.

[6] Secure authentication database.

Client SADB calculator 110 prompts user 114 for its SADB password 124, which user 114 enters into the client 102. Ex. 1005, 7:27–29. User 114 enters the received challenge into client SADB calculator 110. *Id.* at 7:29–30. Client SADB calculator 110 generates, via SHA[7] 128, response 130 using challenge 126, SADB password 124, and locally stored serial number 122. *Id.* at 7:34–37. Client 110 transmits response 130 to server 104. *Id.* at 7:37–38. Server SADB calculator 116 employs a compare routine 132 to compare receive response 130 with the response 130[8] locally generated by the server 104. *Id.* at 7:38–41. Server 104 provides client 102 with a message indicating whether the authentication succeeded or failed, and enables appropriate access if successful. *Id.* at 7:42–44.

b) Sormunen (Ex. 1018)

Sormunen is a Patent Cooperation Treaty application published August 28, 1997. Ex. 1018, code (43). Petitioner asserts that Sormunen is prior art under pre-AIA 35 U.S.C. § 102(b). Pet. 1.

Sormunen's "invention relates to 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. 1008, 1:3–5. Sormunen discloses the use of mobile communication systems including cellular systems, paging systems, and mobile phone systems. *Id.* at 4:36–5:1. User information is transmitted in enciphered[] electronic form and the receiver can be recognized in order to prevent abuse." *Id.* at 6:7–9.

---

[7] Secure hashing algorithm.

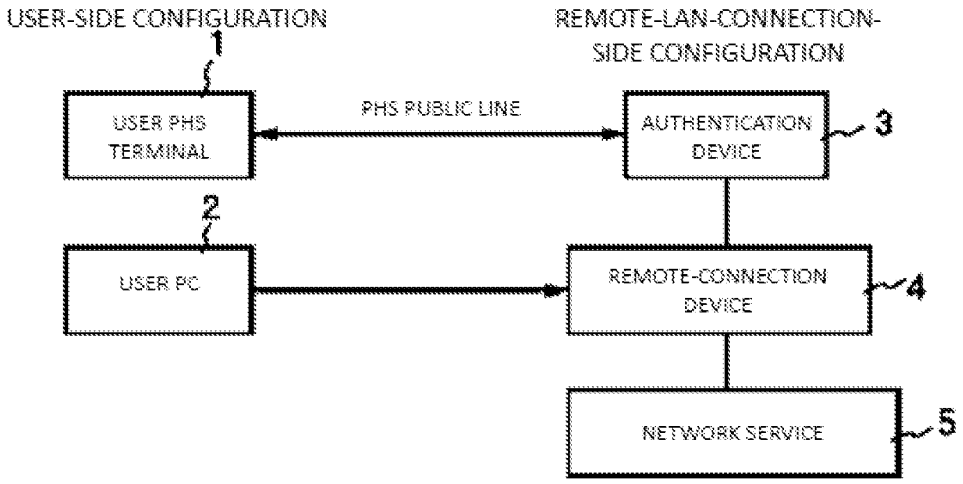
[8] We note the use of reference numeral 103 in reference to the received response and the locally generated response. Despite the use of the same reference numeral, we understand the received response and the locally generated response to be different elements of the disclosed invention.

c) Katou (Ex. 1006)

Katou is a Patent Cooperation Treaty application published January 14, 2000. Ex. 1006, code (43). Petitioner asserts that Katou is prior art under pre-AIA 35 U.S.C. § 102(a). Pet. 1.

Katou relates to "an authentication system and an authentication device that permits the provision of a local area network (LAN) service only to proper users. Ex. 1006 ¶ 2. Fig. 1, reproduced below, "is a block diagram of one embodiment of [the] authentication system." *Id.* ¶ 12.

FIG. 1



As shown in Figure 1, authentication device 3 is a device that verifies the validity of a user and performs: management of a user-password request/notification function; issuance of a temporary password in response to a connection request from the user; and notification of the temporary password to user PHS terminal 1 and remote-connection device 4. Ex. 1006 ¶ 13. "Based on the 'temporary password' issued by the authentication device 3, the remote-connection device 4 accepts the connection request

from the user PC 2, which is a computer system for user connection, and remotely connects a proper user or an inquiring user to the authentication device 3." *Id.* ¶ 14. User Personal Handy-phone System (PHS) terminal 1 is a commercially available simplified mobile telephone having a user-password request/notification function. *Id.* If a user makes a request to authentication device 3 for a temporary password and the user is properly authenticated, then authentication device 3 gives notification of the temporary password. *Id.*

3. Ground 1: Alleged Obviousness of Claims 1–3 and 5–7 Based on the Combined Teachings of Guthrie and Sormunen

For this Ground, Patent Owner contests Petitioner's reasoning in support of the proposed combination. Prelim. Resp. 15–20. As our determination with respect to Petitioner's reasoning is dispositive for this Ground, we focus our discussion on that reasoning and Patent Owner's arguments pertaining to it.

Petitioner asserts that a "POSITA would have found it obvious to implement Sormunen's mobile station and method for requesting and obtaining authentication data at the mobile station in Guthrie's authentication system to further improve security." Pet. 10. Petitioner articulates three reasons in support of its assertion. Patent Owner disagrees with Petitioner's reasoning. Prelim. Resp. 15–20. We discuss each of Petitioner's articulated reasons in turn.

a) First Reason

Petitioner asserts that "because Sormunen recognizes that cellular networks and SMS messaging are more secure than computer networks like the Internet, a POSITA would have been motivated to implement

Sormunen's mobile station in Guthrie to request and receive Guthrie's challenge to prevent the challenge from being exposed over the computer network." Pet. 10. Petitioner asserts further that "Sormunen teaches that 'unauthorized persons can easily read information transferred via the Internet.'" *Id.* at 10–11 (citing Ex. 1018, 3:4–5).[9] Based on these assertions, Petitioner reasons that "[i]mplementing Sormunen's method of obtaining authentication data in short messages over a mobile communication network in Guthrie would have reduced the risk of exposing the challenge to an unauthorized user and improved security because 'it is almost impossible for outsiders to decipher the content of the short messages.'" *Id.* at 11 (citing Ex. 1018, 6:5–9; Ex. 1002 ¶ 64).

Patent Owner contends that Petitioner's first articulated reason for the proposed combination fails because "*Sormunen* does not recognize that cellular networks and SMS messaging are more secure than computer networks." Prelim. Resp. 16. According to Patent Owner, "*Sormunen* states that unenciphered data (i.e., nonencrypted data) can be read when transmitted over the Internet" and "that SMS messages sent 'in enciphered form' (i.e., encrypted) are 'almost impossible for outsiders to decipher.'" *Id.* (citing Ex. 1018, 3:4–5, 6:5–9). Patent Owner further notes that "*Sormunen* states that its system can be implemented over an Internet connection." *Id.* at 16–17 (citing Ex. 1018, 6:12–17; 6:38–7:4) (internal quotations omitted).

We agree with Patent Owner that Petitioner's first articulated reason in support of the proposed combination lacks rational underpinning because

[9] Here and throughout the remainder of this Decision, citations to references that are not the basis for the challenge being discussed are omitted.

Sormunen does not support the premise that cellular networks and SMS messaging are more secure than computer networks.

b) Second Reason

Petitioner asserts that "a POSITA would have recognized that maintaining Guthrie's never-transmitted secret password, unlike Sormunen's authentication data that is all transmitted over one network or another, would result in a more secure combined system." Pet. 11. According to Petitioner, the combined system would ensure "that an unauthorized user in possession of the mobile station and challenge cannot access the secured system without the user's secret password." *Id.* at 11–12 (citing Ex. 1002 ¶ 65).

Patent Owner contends that "*Guthrie* already does not transmit the user's password," "[s]o combining *Sormunen* with *Guthrie* does not address any alleged deficiency in *Guthrie*." Prelim. Resp. 18 (citing Ex. 1007, 4:23–27, 6:10–27, Fig. 3).

Although we are unaware of any requirement that a secondary reference, such as Sormunen, need address an alleged deficiency in a base reference, such as Guthrie, in order to demonstrate obviousness, we agree with Patent Owner that Petitioner's second articulated reason in support of the proposed combination lacks rational underpinning, in that Petitioner's reasoning appears to support the idea that Sormunen's teachings should not be applied to Guthrie. Further, it appears that Petitioner's second reason is not so much an articulation of reasons to combine the references as it is further explanation of the proposed combination.

c) Third Reason

Petitioner asserts that "using Sormunen's mobile station to request and receive Guthrie's challenge further improves security by additionally

verifying the user by their personal communication device." Pet. 12. Petitioner asserts further that "[t]he only user-specific data Guthrie requires for requesting the challenge is the user account ID" and that a "user account ID is typically not secret and can be known to an unauthorized user." *Id.* (citing Ex. 1007, 1:25–29, 7:60–63).

In addition, Petitioner asserts that "[u]sing Sormunen's mobile station to obtain Guthrie's challenge allows the challenge request to be sent from a user-associated mobile station (by a telephone number). This allows Guthrie's server to identify the user based on the mobile station in addition to the user account ID." *Id.* at 12–13 (citing Ex. 1018, 4:30–33, 9:28–32). Petitioner asserts further that "requiring all three components of the combination—a mobile station, a secret password, and a challenge—results in a more secure system than either Guthrie or Sormunen individually." *Id.* at 13 (citing Ex. 1002 ¶ 66).

Patent Owner contends that "Petitioners fail to identify any evidence that requesting a challenge via a mobile station is more secure than requesting it via user account ID." Prelim. Resp. 19 (citing Pet. 12). Patent Owner further contends that "the declaration of Dr. Reiher should be afforded no weigh for this argument because the declaration does nothing more [than] restate Petitioners' argument without any additional supporting evidence or reasoning." *Id.* at 19–20 (comparing Pet. 12–13 to Ex. 1002 ¶ 66; citing *Xerox Corp., et al. v. Bytemark, Inc.*, IPR2022-00624, Paper 9, pp. 15–16 (PTAB Aug. 24, 2022) (Precedential)).

We agree with Patent Owner that Petitioner does not provide adequate support for its assertion that challenge requests via mobile station are more secure than challenge requests that rely on a user account ID. Petitioner

identifies no such teaching in Guthrie or Sormunen. Further, we agree with Patent Owner that Dr. Reiher's testimony amounts to no more than a restatement of Petitioner's argument in the Petition without the support of additional evidence. We, therefore, give this testimony little weight. *Xerox*, IPR2022-00624, Paper 9 at 15–16.

d) Conclusion re Ground 1

For the reasons discussed above, we determine that Petitioner's articulated reasoning in support of the proposed combination that forms the basis of this challenge lacks rational underpinning. Accordingly, Petitioner fails to demonstrate a reasonable likelihood of prevailing for any claim on this ground.

4. Ground 2: Alleged Obviousness of Claims 1–3 and 5–7 Based on the Combined Teachings of Katou and Guthrie

For this Ground, Patent Owner contests Petitioner's reasoning in support of the proposed combination. Prelim. Resp. 27–33. As our determination with respect to Petitioner's reasoning is dispositive for this Ground, we focus our discussion on that reasoning and Patent Owner's arguments pertaining to it.

Petitioner asserts that a "POSITA would have found it obvious to add Guthrie's challenge-response process to [Katou's] three-device architecture, in place of [Katou's] singular temporary password, to further improve security." Pet. 59.

Petitioner asserts that a "POSITA would have been motivated to incorporate Guthrie's challenge-response process into [Katou] to enhance [Katou's] security by preventing the user's secret password from being exposed during transmission." Pet. 60.

Patent Owner contends that "[*Katou*] does not contemplate that data such as the temporary password might be intercepted while being transmitted to the mobile device—in fact, [*Katou*] boasts that its authentication system provides 'extremely strong security' and that it would be 'extremely difficult for a third party to improperly use the network service.'" Prelim. Resp. 32 (citing Ex. 1005 ¶ 22). Thus, according to Patent Owner, "a POSITA would not be motivated to incorporate *Guthrie* or any other reference into [*Katou*] to improve the [*Katou*] system's security."

Although we do not agree with Patent Owner that Katou's statements about the strength of its security preclude improvement of that security, we agree with Patent Owner that Petitioner's reasoning is flawed because Katou does not contemplate transmitting the user's secret password. Rather, Katou describes a system that issues a temporary password upon request for user authentication. *See*, *e.g.*, Ex. 1005, Abs. Moreover, Petitioner has not adequately explained how Guthrie's hashing algorithm and challenge-response process would be implemented in Katou's system.

Petitioner's further reasoning that a "POSITA would have been motivated to incorporate Guthrie's challenge-response process into [Katou], in place of Kato's temporary password, to further enhance [Katou's] security by only transmitting the challenge . . . , preventing exposure of the password, and by requiring the user's secret password in addition to the challenge to obtain the response" suffers from the same deficiencies.

For these reasons, we determine that Petitioner has not demonstrated a reasonable likelihood of prevailing for any claim on this ground.

III. CONCLUSION

For the foregoing reasons, the Petition fails to demonstrate a reasonable likelihood of prevailing in showing the unpatentability of at least one of the challenged claims of the '658 Patent.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the Petition is denied, and no trial is instituted.

FOR PETITIONER:

Lionel M. Lavenue
Kara A. Specht
Cory Bell
Xirui Zhang
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP
lionel.lavenue@finnegan.com
kara.specht@finnegan.com
cory.bell@finnegan.com
xirui.zhang@finnegan.com

For PATENT OWNER:

John Wittenzellner
Todd Landis
Michael Fagan
Mark McCarthy
WILLIAMS SIMONS & LANDIS PLLC
johnw@wsltrial.com
tlandis@wsltrial.com
mfagan@wsltrial.com
mmccarthy@wsltrial.com

Trials@uspto.gov
571-272-7822

Paper 9
Date: July 18, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, LLC,
Petitioner,

v.

DYNAPASS IP HOLDINGS LLC,
Patent Owner.

IPR2023-00425
Patent 6,993,658 B1

Before KEVIN F. TURNER, KRISTEN L. DROESCH, and LYNNE H. BROWNE, *Administrative Patent Judges.*

BROWNE, *Administrative Patent Judge.*

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314, 37 C.F.R. § 42.4

I. INTRODUCTION

Unified Patents, LLC ("Petitioner") filed a Petition (Paper 1 ("Pet.")) requesting institution of an *inter partes* review of claims 1 and 3–6 of U.S. Patent No. 6,993,658 B1 (Ex. 1001, "the '658 Patent"). Dynapass IP Holdings LLC ("Patent Owner") timely filed a Preliminary Response. Paper 8 ("Prelim. Resp.").

Under 35 U.S.C. § 314(a), an *inter partes* review may not be instituted unless the information presented in the Petition and any response thereto shows "there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." Upon consideration of the Petition and the evidence of record, we conclude that the information presented in the Petition establishes that there is a reasonable likelihood that Petitioner would prevail in challenging at least one of claims 1 and 3–6 of the '658 Patent as unpatentable under the grounds presented in the Petition. Pursuant to § 314, we hereby institute an *inter partes* review as to the challenged claims of the '658 Patent.

A. Real Parties in Interest

Petitioner identifies itself, Unified Patents, LLC, as the only real party-in-interest. Pet. 79. Patent Owner identifies itself, Dynapass IP Holdings LLC and DynaPass Inc., as the only real parties-in-interest. Paper 3, 1.

B. Related Matters

The parties identify the following as related district court matters: *Dynapass IP Holdings LLC v. Regions Financial Corporation*, 2:22-cv-00215 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. JPMorgan Chase & Co.*, 2:22-cv-00212 (EDTX 6-17-2022), *Dynapass IP Holdings LLC*

v. PlainsCapital Bank, 2:22-cv-00213 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Woodforest National Bank*, 2:22-cv-00218 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Bank of America Corporation*, 2:22-cv-00210 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Wells Fargo & Company*, 2:22-cv-00217 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Truist Financial Corporation*, 2:22-cv-00216 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. PNC Financial Services*, 2:22-cv-00214 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. BOKF, National Association*, 2:22-cv-00211 (EDTX 6-17-2022), *Dynapass Inc. v. Mobile Authentication Corporation*, 8:18-cv-01173 (C.D. Cal. 7-3-2018). Pet. 80–81; Paper 3, 1–2.

Patent Owner also identifies *Bank of America, N.A. v. Dynapass IP Holdings LLC*, IPR2023-00367 (filed January 3, 2022) as a related matter. Paper 3, 2.

C. The '658 Patent

The '658 Patent is titled "Use of Personal Communication Devices For User Authentication." Ex. 1001, code (54). The invention "relates generally to the authentication of users of secure systems and, more particularly, the invention relates to a system through which user tokens required for user authentication are supplied through personal communication devices such as mobile telephones and pagers." *Id.* at 1:7–11.

One embodiment of the invention provides a password setting system that includes a user token server and a communication module wherein a user token server generates a random token in response to a request for a new password from a user. Ex. 1001, 1:63–2:2. "The server creates a new

password by concatenating a secret passcode that is known to the user with the token" and "sets the password associated with the user's user ID to be the new password." *Id.* at 2:2–6. A "communication module transmits the token to a personal communication device, such as a mobile phone or a pager carried by the user." *Id.* at 2:6–8. Then, the user concatenates the secret passcode with the received token in order to form a valid password, which the user submits to gain access to the secure system. *Id.* at 2:8–11.

Figure, reproduced below, "illustrates an overview, including system components, of a user authentication system 100 according to a preferred embodiment of the present invention." Ex. 1001, 4:2–4.

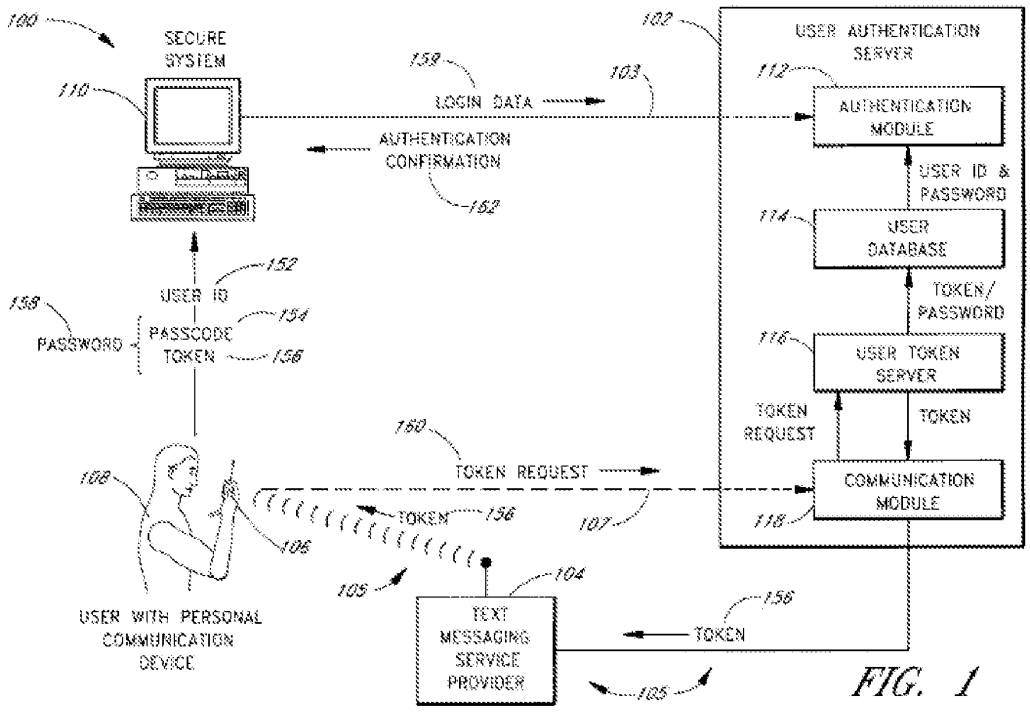


FIG. 1

User authentication system 100 includes authentication Server 102, text messaging Service provider 104, personal communication device 106 carried

by user 108, and secure system 110 to which the authentication system 100 regulates access. *Id.* at 4:9–13. "[P]ersonal communication device 106 is preferably a pager or a mobile phone having SMS (short message Service) receive capability." *Id.* at 4:13–15. Secure system 110 can be "any system, device, account, or area to which it is desired to limit access to authenticated users." *Id.* at 4:18–20.

User authentication server 102 is configured to require that user 108 supply authentication information through secure system 110 in order to gain access to secure system 110. Ex. 1001, 4:32–35. Authentication information provided by the user includes user ID 152, passcode 154 and user token 156. *Id.* at 4:36–37. User ID 152 may be publicly known and used to identify the user and passcode 154 is secret and only known to the user 108, whereas token 156 is provided only to user 108 by user authentication server 102 through personal communication device 106. *Id.* at 4:39–44. To gain access to secure system 100, user 108 combines token 156 with passcode 154 to form password 158. *Id.* at 4:52–53. Thus, user 108 needs to have personal communication device 106 in order to gain access to secure system 110. *Id.* at 4:46–48. Further, token 156 has a limited lifespan, such as 1 minute or 1 day. *Id.* at 4:44–45.

D. Challenged Claims

Petitioner challenges claims 1 and 3–6. Pet. 1. Claims 1 and 5, reproduced below with Petitioner's identifiers included, are the independent claims at issue in this proceeding. Ex. 1001, 11:43–12:13, 12:20–47. Claims 3 and 4 depend from claim 1 and claim 6 depends from claim 5. *Id.* at 12:16–19, 12:48–52.

1. [1.0] 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:

[1.1] 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;

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

[1.3] 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;

[1.4] setting a password associated with the user to be the new password;

[1.5] activating access the user account on the first secure computer network;

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

[1.7] receiving the password from the user via the first secure computer network, and

[1.8] 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.

5. [5.0] A user authentication system comprising:

[5.1] a computer processor,

[5.2] 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;

> [5.3] 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;
>
> [5.4] a communication module configured to transmit the token to the personal communication device through the cell phone network, and
>
> [5.5] 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, [5.6] 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.

Ex. 1001, 11:43–12:13, 12:20–47.

E. Prior Art and Asserted Grounds

Petitioner asserts that claims 1 and 3–6 would have been unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
5	103	Veneklase,[1] Jonsson[2]
1, 3–6	103	Kew,[3] Sormunen[4]

[1] EP 0 844 551 A2, published May 27, 1998 ("Veneklase") (Ex. 1005).
[2] WO 96/00485, published January 4, 1996 ("Jonsson") (Ex. 1006).
[3] WO 95/19593, published July 20, 1995 ("Kew") (Ex. 1007).
[4] WO 97/31306, published August 28, 1997 ("Sormunen") (Ex. 1008).

II. ANALYSIS

A. Level of Ordinary Skill in the Art

In determining the level of skill in the art, we consider the type of problems encountered in the art, the prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level of active workers in the field. *Custom Accessories, Inc. v. Jeffrey-Allan Indus. Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986); *Orthopedic Equip. Co. v. U.S.*, 702 F.2d 1005, 1011 (Fed. Cir. 1983).

Petitioner contends that a person of ordinary skill in the art ("POSITA[5]") "for 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. EX1001, generally; EX1003, ¶¶49-51." Pet. 5. "For the purposes of [the Preliminary] Response only, Patent Owner does not dispute the level of skill of a person of ordinary skill in the art ('POSITA') identified in the Petition." Prelim. Resp. 11.

Based on the record presented, including our review of the '658 Patent and the types of problems and solutions described in the patent and the cited prior art, we adopt Petitioner's assessment of the level of ordinary skill in the art and apply it for purposes of this Decision.

B. Claim Construction

We apply the claim construction standard articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc), and its progeny.

---

[5] Person of ordinary skill in the art.

Only terms that are in controversy need to be construed, and then only to the extent necessary to resolve the controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Matal*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (in the context of an *inter partes* review, applying *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

Petitioner states that "all terms should be given their plain meaning." Pet. 6. Yet, Petitioner proposes claim construction for "cell phone network" and "[n]ot known to the user." Pet. 9–13.[6]

"Patent Owner contends that claim construction is not necessary for the Board to determine that the Petition fails to demonstrate a reasonable likelihood that any challenged claim of the '658 Patent is unpatentable." Prelim. Resp. 11.

At this stage of this proceeding, we agree with the parties that claim construction is not necessary.

C. Patentability Challenges

1. Principles of Law: Obviousness

A claim is unpatentable under 35 U.S.C. § 103 if "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art;

[6] Petitioner also acknowledges that the Board may construe some limitations as means-plus-function limitations. Pet. 6.

(3) the level of skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations.[7] *See Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17–18 (1966).

2. Prior Art

a) Veneklase (Ex. 1005)

Veneklase is a European Patent application published May 27, 1998. Petitioner asserts that Veneklase is prior art under pre-AIA 35 U.S.C. § 102(a) and (b). Pet. 1.

Veneklase's "invention relates to a security and/or access restriction system . . . adapted to grant only authorized users access to a computer system and/or certain data." Ex. 1005, 1:5–9. Veneklase is directed to preventing exposure and hacking of user passwords (*id.* at 2:2–21), theft of user access cards (*id.* at 2:22–37), and interception and decryption of encryption of keys (*id.* at 2:37-57). The invention provides "a technique to substantially prevent the unauthorized interception and use of transmitted data . . . by splitting the data into a plurality of separate communication channels, each of which must be 'broken' for the entire data stream to be obtained." *Id.* at 3:3–11.

In Veneklase's system individual 18, desiring access to and within computer 80, utilizes a first communication channel 82 (e.g., a first telephone line, radio channel, and/or satellite channel) and communicates, by use of his or her voice or by use of a computer 19, a first password to analyzing means 12. *Id.* at 6:5–10. "Analyzing means 12 then checks and/or compares this first received password with a master password list

[7] The current record does not present or address any evidence of nonobviousness.

which contains all of the authorized passwords associated with authorized entry and/or access to computer 80." *Id.* at 6:10–14. If the received password matches an entry of the master password list, analyzing means 12 causes the random code generation means 14 to generate a pseudo-random number or code and to transmit the number and/or code via a second communications channel 84, to the individual 85 associated with the received password 202 in the master password list. *Id.* at 6:27–37. "Once the pseudo-random number is received by the analyzing means 12, from channel 82, it is compared with the number generated by generation means 14." *Id.* at 6:51–54. If the two codes are substantially the same, entry to computer 80 or to a certain part of computer 80 such as the hardware, software, or firmware portions of computer 80 is granted to individual 18. *Id.* at 6:54–58.

b) Jonsson (Ex. 1006)

Jonsson is a Patent Cooperation Treaty application published January 4, 1996. Petitioner asserts that Jonsson is prior art under pre-AIA 35 U.S.C. § 102(a) and (b). Pet. 1.

Jonsson provides an authentication procedure wherein the user carries a personal unit not limited to use with or physically connected to a terminal of any one specific electronic service. Ex. 1006, 2:30–34. Jonsson's personal unit includes a receiver for receiving a transmitted challenge code and an algorithm unit which processes the challenge code, a user input such as a personal identification number (PIN) or electronically recognizable signature, and an internally stored security key for calculating a response code according to a pre-stored algorithm. Ex. 1006 at 6:24–29.

c) Kew (Ex. 1007)

Kew is a Patent Cooperation Treaty application published July 20, 1995. Petitioner asserts that Kew is prior art under pre-AIA 35 U.S.C. § 102(a) and (b). Pet. 1.

Kew's invention relates to a method for "preventing unauthorized access to a host computer system." Ex. 1007, 1:3–5. Specifically, Kew describes a "method of preventing unauthorized access to a host computer system by a user at a remote terminal." *Id.* at 1:21–23. In Kew's method the host computer system accepts a user identification code input to the terminal by the user and generates a random code (Code A). *Id.* at 1:24–26. Using a transformation algorithm, Kew's computer system transforms Code A to transformed Code B. *Id.* at 1:27–30. The computer system also transmits Code A to user's receiver which transform's Code A to transformed Code C. *Id.* at 1:31–34. The user inputs Code C into the remote terminal and the computer system compares Code B with Code C, and if the Codes match permits access to the host computer system. *Id.* at 1:36–2:3.

d) Sormunen (Ex. 1008)

Sormunen is a Patent Cooperation Treaty application published August 28, 1998. Petitioner asserts that Sormunen is prior art under pre-AIA 35 U.S.C. § 102(a) and (b). Pet. 1.

Sormunen's "invention relates to 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. 1008, 1:3–5. Sormunen discloses the use of mobile communication systems including cellular systems, paging systems, and mobile phone systems. *Id.* at 4:36–5:1.

3. Ground 1: Alleged Obviousness of Independent Claim 5

Petitioner asserts that claim 5 is unpatentable over the combined teachings of Veneklase and Jonsson. Pet. 13. Petitioner addresses each limitation of claim 5 and provides the testimony of Dr. McNair in support of its position with respect to them claim 5. Pet. 17–46; Ex. 1003 ¶¶ 71–111. Patent Owner does not contest Petitioner's assertions for limitations [5.0]–[5.2] of claim 5. For the uncontested limitations ([5.0]–[5.2]), we have considered Petitioner's evidence and arguments with respect to these limitations, including the relevant testimony of Dr. McNair and find it to be sufficient to show that Petitioner has demonstrated a reasonable likelihood of prevailing in showing that Veneklase, either alone or in combination with Jonsson, teaches or suggests these limitations. Accordingly, we focus our discussion on contested limitations [5.3]–[5.6] and Patent Owner's arguments regarding these limitations.

a) Limitation [5.3]: 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;

Petitioner asserts that "*Veneklase* in combination with *Jonsson* teaches this limitation." Pet. 26 (citing Ex. 1003 ¶¶ 83–90). Regarding Veneklase, Petitioner asserts that Veneklase discloses assigning a password to the user; receiving the password by use of a first communication channel; generating a code in response to the received password; transmitting the code to the user via a second communications channel; transmitting the code to the computer; and allowing access to the computer only after the code is transmitted to the computer. Pet. 26 (citing Ex. 1005, 4:8–15).

Specifically, Petitioner asserts that "*Veneklase* discloses a user/password check module (i.e., a control module) located on the host computer system 402 (i.e., the computer processor)" and that the "user/password check module assigns two passwords, one that is known to the user and one that is not previously known to the user." Pet. 26–27 (citing Ex. 1005, Fig. 6).[8] Petitioner asserts further that "[w]hile *Veneklase* teaches an authentication system in which the user inputs both a token that is not known to the user beforehand (e.g., the random code) and a passcode that is known to the user (e.g., the received password), it does not disclose creating a new password based on those two items." *Id.* at 28.

Turning to Jonsson, Petitioner asserts that Jonsson discloses an authentication 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'" and that "[t]his challenge code generated by the system is a *token* because it is not known to the user before it is generated and sent to the user." Pet. 28 (citing Ex. 1006, 4:24–5:6; Ex. 1003 ¶¶ 86–87). Petitioner asserts further that "*Jonsson* discloses the use of a 'user input such as a personal identification number (PIN),' which by its very nature of being a user defined input, is known to the user beforehand" and that "*Jonsson* discloses an algorithm that '**calculates a response code [e.g., new password] based on the received challenge code [e.g., token], the user input (e.g., PIN) [e.g., passcode]**, and optionally [a] secret key.'" Pet. 29 (citing Ex. 1006, 3:3–10, 7:5–10, 8:12–14, 9:23–25).

---

[8] Here and for the remainder of this decision, we do not reproduce the colored font used in the Petition.

Petitioner asserts that it would have been obvious to combine Veneklase's token and passcode to "create a new password based on both of them." *Id.* at 28. Petitioner then asserts that "*Veneklase*'s authentication system would incorporate *Jonsson*'s teachings related to using an algorithm to create a new password (e.g., response code) based on a known passcode (e.g., the received password/PIN) and an unknown token (e.g., the random code/challenge code)." *Id.* at 30 (citing Ex. 1003 ¶¶ 83–89). Thus, according to Petitioner,

> *Veneklase* in combination with *Jonsson* teaches *a control module* (e.g., user/password check module) *executed on the computer processor configured to create a new password* (e.g., assigning a password to the user) *based at least upon a token* (e.g., random code) *and a passcode* (e.g., received password), *wherein the token is not known to the user* (e.g., generated by the system) *and wherein the passcode is known to the user* (e.g., received from the user), *the control module further configured to set a password associated with the user to be the new password* (e.g., set an expected response code).

Id. (citing Ex. 1003 ¶¶ 83–90).

In support of these assertions, Petitioner reasons that "[a] POSITA would have been motivated to make such a combination because having only the one password transmitted via the computer system is more efficient and secure." Pet. 31 (citing Ex. 1003 ¶ 91). According to Petitioner, "*Veneklase*'s system allows for authentication through user input of a known and unknown code at separate times in a two-step process, while a POSITA would look to *Jonsson* because it would provide the added benefit of reducing the steps to a single step and thus reducing the amount of time required for the authentication process." *Id.* Petitioner reasons further that "a POSITA would have been motivated to make such a combination because

implementing *Veneklase*'s authentication system with the algorithm of *Jonsson*'s system provides an additional layer of security." *Id.* at 31–32.

In addition, Petitioner asserts that Veneklase "explicitly discloses embodiments in which data streams are encoded and decoded using algorithms for additional security." Pet. 32 (citing Ex. 1005, 9:26–10:11; *KSR*, 550 U.S. at 418–419). Thus, according to Petitioner, "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, such as described in *Jonsson*, to provide additional security." *Id.* (citing Ex. 1003 ¶ 92). And, Petitioner asserts that "[a] POSITA would further be motivated to combine *Veneklase* and *Jonsson* because the combination merely uses a known technique to improve similar devices in the same way." *Id.* at 33 (citing *KSR* 550 U.S. at 401).

Patent Owner contends that "modifying *Veneklase's* system by abolishing the two-step authentication process, as proposed by Petitioner, would violate *Veneklase's* principle of operation." Prelim. Resp. 17. According to Patent Owner, "this two-step authentication process is a key feature of *Veneklase's* principle of operation, and a POSITA would not seek to remove steps as Petitioner proposes." *Id.* (citing Ex. 1005, 7:16–28). Patent Owner contends that "the proposed modification of *Veneklase* is far too drastic to be considered obvious, and thus the combination of *Veneklase* and *Jonsson* fails to render claim 5 obvious." *Id.* at 18 (citing MPEP § 2143.01(VI); *Plas-Pak Indus. v. Sulzer Mixpac AG*, 600 F. App'x. 755, 758 (Fed. Cir. 2015)).

We disagree with Patent Owner's arguments. Veneklase is directed to "a security and/or access restriction system . . . which is adapted to grant only

authorized users access to a computer system and/or to certain data which may be resident within the computer system and/or resident within a communications channel and/or other communications medium." Ex. 1005, 1:5–12. Patent Owner has not adequately demonstrated that the two-step authentication process is a key feature of Veneklase's principle of operation such that the proposed modification would render Veneklase's system inoperable. Rather, Patent Owner relies on unsupported attorney argument. *See* PO Resp. 17–18.

Incorporating Jonsson's teachings related to using an algorithm to create a new password would not destroy the principle of operation of Veneklase's security system because it only changes how Veneklase accomplishes its goal of preventing unauthorized access to a computer system, rather than defeating its goal of preventing such access. *See In re Mouttet*, 686 F. 3d 1322, 1332 (Fed. Cir. 2012). Further, we do not agree that *Plas-Pak* (a nonprecedential decision) supports the Patent Owner's contention that the proposed combination impermissibly changes Veneklase's principle of operation as Patent Owner has not identified differences between the two authentication processes that would be "unlikely to motivate a person of ordinary skill to pursue" the proposed combination. *Plas-Plak*, 600 F. App'x at 757-59.

Patent Owner contends that "Petitioner provides zero evidence that the security of its proposed combination is superior to the existing multi-layer/level security in *Veneklase*." Prelim. Resp. 19. Thus, according to Patent Owner, "there is no motivation to combine *Veneklase* and *Jonsson*." *Id.* at 20.

We disagree with Patent Owner's arguments. Petitioner does not propose modifying Veneklase to include Jonsson's teachings solely because the security of the proposed combination is superior to the security in Veneklase. Rather, Petitioner asserts that "[a] POSITA would have been motivated to make such a combination because having only the one password transmitted via the computer system is more *efficient* and secure." Pet. 31 (citing Ex. 1003 ¶ 91). The Petition explains how the combination is more efficient in that it requires only a single step which reduces the amount of time required for the authentication process. *Id.* Moreover, the Petition explains how the proposed combination is more secure than Veneklase's system in that it prevents unauthorized persons from accessing the computer system by engaging in SIM swapping. *Id.* at 32.

Patent Owner contends that the portion of Veneklase cited by Petitioner in support of its assertion that Veneklase provides explicit motivation for using Jonsson's algorithm in Veneklase's system "does not pertain to an algorithm." Prelim. Resp. 20 (citing Pet. 32 (citing Ex. 1005, 9:20–10:11)).

We disagree with Patent Owner's argument. Petitioner asserts that Veneklase "explicitly discloses embodiments in which data streams are encoded and decoded using algorithms for additional security." Pet. 32 (citing Ex. 1005, 9:26–10:11). The cited portion of Exhibit 1005 discloses, in relevant part, that

> System 70, as further shown, includes a data stream dividing means 74 which in one embodiment comprises a commercially available one input and two channel output time division or statistical multiplexor which samples the bits of received data and places, in a certain predetermined manner (e.g. alternately) some of the received data bits onto the first communications

> channel 76 and some of the received data bits onto the second communications channel 78. In this manner, one attempting to wrongfully intercept and/or access the data stream 72 would need access to both communications channels 76, 78 and would need to know the dividing *algorithm* that dividing means 74 utilizes to divide the received data for placement onto channels 76,78.

Ex. 1005, 9:33–48.

The cited portion further states, in relevant part, that

> security system 70 further includes a decoding means 88 which may comprise a commercially available microprocessor operating under stored algorithmic program control and which contains "mirror image" of the *algorithm* used to divide the data stream transmitted to it by means 74. In this manner, the data from each of the channels 76,78 is reconstituted onto single channel 89, in substantially the exact same manner that it was received by means 74.

Id. at 9:50–58.

b) Limitation [5.4]: a communication module configured to transmit the token to the personal communication device through the cell phone network;

Petitioner asserts that "*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.'" Pet. 35 (quoting Ex. 1005, 8:1–5). Petitioner asserts further that "the generated random number code and pager number are 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.'" *Id.* (citing Ex. 1005, 7:52–8:17, Fig. 6).[9]

Thus, according to Petitioner, "*Veneklase* 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)." Pet. 37 (citing Ex. 1003 ¶¶ 97–100). Petitioner asserts that "[a] POSITA would have understood that the 'conventional and commercially available communication channel 422' described in *Veneklase* is the same type of cell phone network disclosed in the '658 patent, which repeatedly makes clear that it covers both networks that communicate with cell phones and those that communicate with pagers." *Id.* at 36

Patent Owner agrees that "*Veneklase*'s system uses the received password (i.e., the first step in the two-step process) to lookup the user's phone number and transmit the randomly generated code to the user." Prelim. Resp. 22–23 (quoting Ex. 1005, 8:2–15; 6:10–37). Noting that "Petitioner's proposed combination includes replacing *Veneklase's* two-step authentication process (i.e., user transmission of *Veneklase's* password, and subsequent user transmission of *Veneklase's* random code) with the single step in *Jonsson* (i.e., user transmission of Jonsson's response code)," Patent Owner contends that "[t]he Petition is silent on how, following the proposed modification to *Veneklase* which abolishes user transmission of *Veneklase's* password, the user's phone number will be identified, and thus how the randomly generated code will be transmitted to the user's pager." *Id.*

[9] The Petition cites Ex. 1006. Veneklase, however, is Ex. 1005.

at 23–24. According to Patent Owner, "[w]ith *Veneklase's* modified system being unable to search the password list for a phone number, and thus unable to transmit the randomly generated code to the user's pager, *Veneklase's* modified system is inoperative," and thus, "there is no motivation for the proposed modification." *Id.* at 24.

We disagree with Patent Owner's characterization of the proposed modification as it pertains to limitation [5.4]. It is our understanding that in the proposed combination the user's device would be identified in accordance with Jonsson's teachings not Veneklase's. *See* Pet. 30–32. In other words, the user's device would be identified in response to the user's request for authentication as described in Jonsson. *See e.g.*, Ex. 1006, 9:2–8; 10:13–27, Fig. 3). Accordingly, the ability to look up the user's phone number is not a requirement of the combination and Patent Owner's argument is inapposite.

> c) *Limitation [5.5]: 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,*

Petitioner asserts that "[i]n the combination with *Jonsson* discussed with respect to element [5.3], a POSITA would have understood that the new password . . . being sent back to computer 402 and compared against the expected value is the one created by the algorithm based on both the known passcode . . . and the randomly generated token." Pet. 38 (citing Ex. 1003 ¶¶ 83–89). Petitioner asserts further that "*Veneklase* discloses that [the] communication in which the user submits its credentials to the host computer and the initial sending of the random code to the personal device '**utilizes two distinct communication channels**.'" *Id.* at 39 (citing

Ex. 1005, 3:50–4:3, 7:11–28). Petitioner also asserts that a "POSITA would have understood that [Veneklase's] communication network is [a] *secure computer network* because the use of the authentication procedures described in *Veneklase* make secure the host computer system." *Id.* at 40 (citing Ex. 1005, 9:3–14; Ex. 1003 ¶¶ 101–104).

Patent Owner contends that Petitioner's assertions "conveniently glosses over the fact that the proposed combination requires modifying *Veneklase's* 'pager 420' to execute an algorithm that 'calculates a response code based on the received challenge code [and] the user input (e.g., PIN),' as performed by Jonsson's 'personal unit 20.'" Prelim. Resp. 26 (citing Ex. 1006, 8:12–14). Patent Owner further contends that "Petitioner presents zero evidence that *Veneklase's* 'pager 420' is capable of executing such an algorithm." *Id.*

We disagree with Patent Owner's arguments. Jonsson explicitly teaches that "the capacity for performing the necessary calculations exists in conventional cellular telephones and personal communication units [(i.e. pagers)], allowing the present invention to be implemented through software." Ex. 1006, 7:27–31. Thus, Jonsson's disclosure provides evidence that pagers, such as Veneklase's pager 420, are capable of executing Jonsson's algorithm.

In addition, Patent Owner contends that "Petitioner's proposed combination also fails to disclose 'an authentication module configured to receive the password from the user through a secure computer network.'" Pet. 27. As best understood, Patent Owner appears to be arguing that in Jonsson's system the password is not "received from the user" because it is not displayed to the user.

The claim language at issue, however, does not require that the password be known to the user. Rather, it requires that it be received from the user (in other words from the user's device). Thus, Patent Owner's argument is unconvincing.

> d) *Limitation [5.6]: 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.*

Petitioner asserts that Veneklase discloses that the user 404 sends a "'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**.'" Pet. 41 (citing Ex. 1005,[10] 6:45–7:10, 8:18–27). Petitioner asserts further that "*Veneklase* discloses an embodiment which 'includes a timer or "timing means" 40 which may comprise one or more software subroutines which are adapted to operate and/or execute within and/or upon computer 80,' such as a watchdog timer." *Id.* at 42 (citing Ex. 1005, 8:28–39).[11]

Petitioner asserts that in the combination with Jonsson "a POSITA would have understood that the new password (e.g., response code) being sent back to computer 402 and compared against the expected value is the one created by the algorithm based on both the known passcode (e.g., PIN)

[10] The Petition cites Ex. 1006; however, Veneklase is Ex. 1005.
[11] *See* note 5.

and the randomly generated token (e.g., challenge code)." Pet. 43 (citing Ex. 1003 ¶¶ 83–89). Thus, according to Petitioner, "the predetermined period would be the time between the receipt of the token (e.g., randomly generated challenge code) and the sending back of the newly created password (e.g., response code)." *Id.*

Turning to the deactivating part of limitation [5.6], Petitioner asserts that "*Veneklase*'s teaching is within the scope of the recited deactivating limitation because it is nearly identical to how this limitation is described in the '658 Patent." Pet. 43.

Patent Owner contends that "neither asserted reference discloses activating an account. And the Petition fails to argue, let alone show, that either reference discloses activating account access in response to generation of the new 'password,' which is 'based at least upon a token and a passcode.'" Prelim. Resp. 30–31 (citing Pet. 41–46). Patent Owner contends further that "[i]nstead, Petitioner incorrectly relies on steps in the prior art that occur well after the claimed 'password' is created." *Id.* at 31.

We disagree with Patent Owner's arguments. Claim 5 requires that the account be activated in response to the password. Ex. 1001, 12:41–43. It does not require that the account be activated in response to creation of the password. *Id.* On the record before us, Petitioner has adequately demonstrated that Veneklase discloses activation of the account in response to the password. *See* Pet. 41–42.

In addition, Patent Owner argues "that 'the predetermined period would be the time between receipt of the token (e.g., randomly generated challenge code) and the sending back of the newly created password (e.g., response code),'" and so, Petitioner's assertion "is flawed on its face because

the claimed 'predetermined amount of time' is the timeframe between activation and deactivation of the account." Prelim. Resp. 31 (citing Ex. 1001, 12:41–45).

We disagree with Patent Owner's argument. Claim 5 requires an authentication module that "deactivates the account within a predetermined amount of time after activating the account." Ex. 1001, 12:43–54). It does not require that the predetermined amount of time correspond to the entire time period between activation and deactivation of the account. On the record before us, Petitioner has adequately demonstrated that Veneklase discloses deactivation of the account within a predetermined amount of time. *See* Pet. 42–43.

e) Conclusion Regarding Ground 1

We have considered Petitioner's evidence and arguments with respect to all limitations of claim 5, including the relevant testimony of Dr. McNair and find it to be sufficient to show that Petitioner has demonstrated a reasonable likelihood of prevailing in showing that Veneklase and Jonsson, either alone or in combination, disclose each limitation of claim 5.

4. Ground 2: Alleged Obviousness of Claims 1 and 3–6

Having determined that Petitioner has demonstrated a reasonable likelihood of prevailing as to claim 5 on the basis of Ground 1, we do not address the patentability challenge on the basis of Ground 2.

III. CONCLUSION

For the foregoing reasons, we are persuaded that the Petition demonstrates a reasonable likelihood of prevailing in showing the unpatentability of at least one of the challenged claims of the '658 Patent. Because Petitioner has satisfied the threshold for institution as to at least one

claim, we institute *inter partes* review on all claims and all grounds raised in the Petition. *See SAS Institute Inc. v. Iancu*, 138 S. Ct. 1348, 1359–60 (2018) (holding that a decision to institute under 35 U.S.C. § 314 may not institute on fewer than all claims challenged in the petition).

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1 and 3–6 of the '658 Patent is instituted with respect to all grounds set forth in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of the '658 Patent shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

FOR PETITIONER:

Jordan M. Rossen
Ashraf Fawzy
UNIFIED PATENTS, LLC
jordan@unifiedpatents.com
afawzy@unifiedpatents.com

For PATENT OWNER:

John Wittenzellner
Todd E. Landis
Michael J. Fagan, Jr.
Mark McCarthy
WILLIAMS SIMONS & LANDIS PLLC
johnw@wsltrial.com
tlandis@wsltrial.com
mfagan@wsltrial.com
mmccarthy@wsltrial.com

Trials@uspto.gov
571-272-7822

Paper 9
Date: July 18, 2023

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, LLC,
Petitioner,

v.

DYNAPASS IP HOLDINGS LLC,
Patent Owner.

IPR2023-00425
Patent 6,993,658 B1

Before KEVIN F. TURNER, KRISTEN L. DROESCH, and LYNNE H. BROWNE, *Administrative Patent Judges.*

BROWNE, *Administrative Patent Judge.*

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314, 37 C.F.R. § 42.4

I. INTRODUCTION

Unified Patents, LLC ("Petitioner") filed a Petition (Paper 1 ("Pet.")) requesting institution of an *inter partes* review of claims 1 and 3–6 of U.S. Patent No. 6,993,658 B1 (Ex. 1001, "the '658 Patent"). Dynapass IP Holdings LLC ("Patent Owner") timely filed a Preliminary Response. Paper 8 ("Prelim. Resp.").

Under 35 U.S.C. § 314(a), an *inter partes* review may not be instituted unless the information presented in the Petition and any response thereto shows "there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." Upon consideration of the Petition and the evidence of record, we conclude that the information presented in the Petition establishes that there is a reasonable likelihood that Petitioner would prevail in challenging at least one of claims 1 and 3–6 of the '658 Patent as unpatentable under the grounds presented in the Petition. Pursuant to § 314, we hereby institute an *inter partes* review as to the challenged claims of the '658 Patent.

A. Real Parties in Interest

Petitioner identifies itself, Unified Patents, LLC, as the only real party-in-interest. Pet. 79. Patent Owner identifies itself, Dynapass IP Holdings LLC and DynaPass Inc., as the only real parties-in-interest. Paper 3, 1.

B. Related Matters

The parties identify the following as related district court matters: *Dynapass IP Holdings LLC v. Regions Financial Corporation*, 2:22-cv-00215 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. JPMorgan Chase & Co.*, 2:22-cv-00212 (EDTX 6-17-2022), *Dynapass IP Holdings LLC*

v. PlainsCapital Bank, 2:22-cv-00213 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Woodforest National Bank*, 2:22-cv-00218 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Bank of America Corporation*, 2:22-cv-00210 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Wells Fargo & Company*, 2:22-cv-00217 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. Truist Financial Corporation*, 2:22-cv-00216 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. PNC Financial Services*, 2:22-cv-00214 (EDTX 6-17-2022), *Dynapass IP Holdings LLC v. BOKF, National Association*, 2:22-cv-00211 (EDTX 6-17-2022), *Dynapass Inc. v. Mobile Authentication Corporation*, 8:18-cv-01173 (C.D. Cal. 7-3-2018). Pet. 80–81; Paper 3, 1–2.

Patent Owner also identifies *Bank of America, N.A. v. Dynapass IP Holdings LLC*, IPR2023-00367 (filed January 3, 2022) as a related matter. Paper 3, 2.

C. The '658 Patent

The '658 Patent is titled "Use of Personal Communication Devices For User Authentication." Ex. 1001, code (54). The invention "relates generally to the authentication of users of secure systems and, more particularly, the invention relates to a system through which user tokens required for user authentication are supplied through personal communication devices such as mobile telephones and pagers." *Id.* at 1:7–11.

One embodiment of the invention provides a password setting system that includes a user token server and a communication module wherein a user token server generates a random token in response to a request for a new password from a user. Ex. 1001, 1:63–2:2. "The server creates a new

password by concatenating a secret passcode that is known to the user with the token" and "sets the password associated with the user's user ID to be the new password." *Id.* at 2:2–6. A "communication module transmits the token to a personal communication device, such as a mobile phone or a pager carried by the user." *Id.* at 2:6–8. Then, the user concatenates the secret passcode with the received token in order to form a valid password, which the user submits to gain access to the secure system. *Id.* at 2:8–11.

Figure, reproduced below, "illustrates an overview, including system components, of a user authentication system 100 according to a preferred embodiment of the present invention." Ex. 1001, 4:2–4.

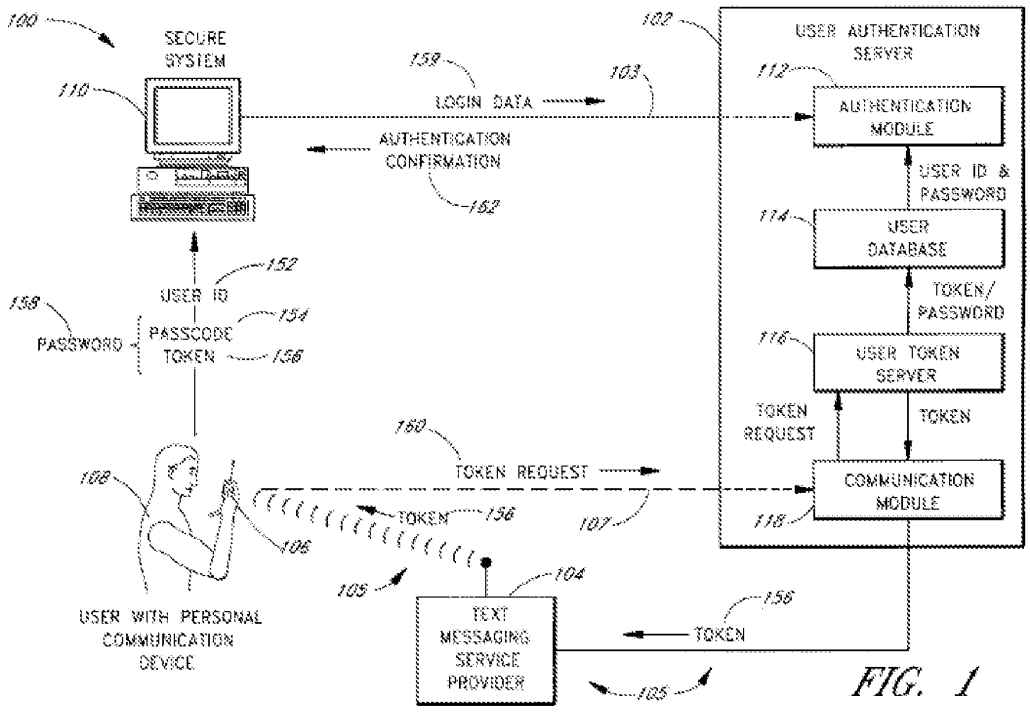


FIG. 1

User authentication system 100 includes authentication Server 102, text messaging Service provider 104, personal communication device 106 carried

by user 108, and secure system 110 to which the authentication system 100 regulates access. *Id.* at 4:9–13. "[P]ersonal communication device 106 is preferably a pager or a mobile phone having SMS (short message Service) receive capability." *Id.* at 4:13–15. Secure system 110 can be "any system, device, account, or area to which it is desired to limit access to authenticated users." *Id.* at 4:18–20.

User authentication server 102 is configured to require that user 108 supply authentication information through secure system 110 in order to gain access to secure system 110. Ex. 1001, 4:32–35. Authentication information provided by the user includes user ID 152, passcode 154 and user token 156. *Id.* at 4:36–37. User ID 152 may be publicly known and used to identify the user and passcode 154 is secret and only known to the user 108, whereas token 156 is provided only to user 108 by user authentication server 102 through personal communication device 106. *Id.* at 4:39–44. To gain access to secure system 100, user 108 combines token 156 with passcode 154 to form password 158. *Id.* at 4:52–53. Thus, user 108 needs to have personal communication device 106 in order to gain access to secure system 110. *Id.* at 4:46–48. Further, token 156 has a limited lifespan, such as 1 minute or 1 day. *Id.* at 4:44–45.

D. Challenged Claims

Petitioner challenges claims 1 and 3–6. Pet. 1. Claims 1 and 5, reproduced below with Petitioner's identifiers included, are the independent claims at issue in this proceeding. Ex. 1001, 11:43–12:13, 12:20–47. Claims 3 and 4 depend from claim 1 and claim 6 depends from claim 5. *Id.* at 12:16–19, 12:48–52.

1. [1.0] 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:

[1.1] 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;

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

[1.3] 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;

[1.4] setting a password associated with the user to be the new password;

[1.5] activating access the user account on the first secure computer network;

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

[1.7] receiving the password from the user via the first secure computer network, and

[1.8] 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.

5. [5.0] A user authentication system comprising:

[5.1] a computer processor,

[5.2] 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;

> [5.3] 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;
>
> [5.4] a communication module configured to transmit the token to the personal communication device through the cell phone network, and
>
> [5.5] 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, [5.6] 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.

Ex. 1001, 11:43–12:13, 12:20–47.

E. Prior Art and Asserted Grounds

Petitioner asserts that claims 1 and 3–6 would have been unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
5	103	Veneklase,[1] Jonsson[2]
1, 3–6	103	Kew,[3] Sormunen[4]

[1] EP 0 844 551 A2, published May 27, 1998 ("Veneklase") (Ex. 1005).
[2] WO 96/00485, published January 4, 1996 ("Jonsson") (Ex. 1006).
[3] WO 95/19593, published July 20, 1995 ("Kew") (Ex. 1007).
[4] WO 97/31306, published August 28, 1997 ("Sormunen") (Ex. 1008).

II. ANALYSIS

A. Level of Ordinary Skill in the Art

In determining the level of skill in the art, we consider the type of problems encountered in the art, the prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level of active workers in the field. *Custom Accessories, Inc. v. Jeffrey-Allan Indus. Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986); *Orthopedic Equip. Co. v. U.S.*, 702 F.2d 1005, 1011 (Fed. Cir. 1983).

Petitioner contends that a person of ordinary skill in the art ("POSITA[5]") "for 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. EX1001, generally; EX1003, ¶¶49-51." Pet. 5. "For the purposes of [the Preliminary] Response only, Patent Owner does not dispute the level of skill of a person of ordinary skill in the art ('POSITA') identified in the Petition." Prelim. Resp. 11.

Based on the record presented, including our review of the '658 Patent and the types of problems and solutions described in the patent and the cited prior art, we adopt Petitioner's assessment of the level of ordinary skill in the art and apply it for purposes of this Decision.

B. Claim Construction

We apply the claim construction standard articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc), and its progeny.

[5] Person of ordinary skill in the art.

Only terms that are in controversy need to be construed, and then only to the extent necessary to resolve the controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Matal*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (in the context of an *inter partes* review, applying *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

Petitioner states that "all terms should be given their plain meaning." Pet. 6. Yet, Petitioner proposes claim construction for "cell phone network" and "[n]ot known to the user." Pet. 9–13.[6]

"Patent Owner contends that claim construction is not necessary for the Board to determine that the Petition fails to demonstrate a reasonable likelihood that any challenged claim of the '658 Patent is unpatentable." Prelim. Resp. 11.

At this stage of this proceeding, we agree with the parties that claim construction is not necessary.

C. Patentability Challenges

1. Principles of Law: Obviousness

A claim is unpatentable under 35 U.S.C. § 103 if "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art;

[6] Petitioner also acknowledges that the Board may construe some limitations as means-plus-function limitations. Pet. 6.

(3) the level of skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations.[7] *See Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17–18 (1966).

2. Prior Art

a) Veneklase (Ex. 1005)

Veneklase is a European Patent application published May 27, 1998. Petitioner asserts that Veneklase is prior art under pre-AIA 35 U.S.C. § 102(a) and (b). Pet. 1.

Veneklase's "invention relates to a security and/or access restriction system . . . adapted to grant only authorized users access to a computer system and/or certain data." Ex. 1005, 1:5–9. Veneklase is directed to preventing exposure and hacking of user passwords (*id.* at 2:2–21), theft of user access cards (*id.* at 2:22–37), and interception and decryption of encryption of keys (*id.* at 2:37-57). The invention provides "a technique to substantially prevent the unauthorized interception and use of transmitted data . . . by splitting the data into a plurality of separate communication channels, each of which must be 'broken' for the entire data stream to be obtained." *Id.* at 3:3–11.

In Veneklase's system individual 18, desiring access to and within computer 80, utilizes a first communication channel 82 (e.g., a first telephone line, radio channel, and/or satellite channel) and communicates, by use of his or her voice or by use of a computer 19, a first password to analyzing means 12. *Id.* at 6:5–10. "Analyzing means 12 then checks and/or compares this first received password with a master password list

[7] The current record does not present or address any evidence of nonobviousness.

which contains all of the authorized passwords associated with authorized entry and/or access to computer 80." *Id.* at 6:10–14. If the received password matches an entry of the master password list, analyzing means 12 causes the random code generation means 14 to generate a pseudo-random number or code and to transmit the number and/or code via a second communications channel 84, to the individual 85 associated with the received password 202 in the master password list. *Id.* at 6:27–37. "Once the pseudo-random number is received by the analyzing means 12, from channel 82, it is compared with the number generated by generation means 14." *Id.* at 6:51–54. If the two codes are substantially the same, entry to computer 80 or to a certain part of computer 80 such as the hardware, software, or firmware portions of computer 80 is granted to individual 18. *Id.* at 6:54–58.

b) Jonsson (Ex. 1006)

Jonsson is a Patent Cooperation Treaty application published January 4, 1996. Petitioner asserts that Jonsson is prior art under pre-AIA 35 U.S.C. § 102(a) and (b). Pet. 1.

Jonsson provides an authentication procedure wherein the user carries a personal unit not limited to use with or physically connected to a terminal of any one specific electronic service. Ex. 1006, 2:30–34. Jonsson's personal unit includes a receiver for receiving a transmitted challenge code and an algorithm unit which processes the challenge code, a user input such as a personal identification number (PIN) or electronically recognizable signature, and an internally stored security key for calculating a response code according to a pre-stored algorithm. Ex. 1006 at 6:24–29.

c) Kew (Ex. 1007)

Kew is a Patent Cooperation Treaty application published July 20, 1995. Petitioner asserts that Kew is prior art under pre-AIA 35 U.S.C. § 102(a) and (b). Pet. 1.

Kew's invention relates to a method for "preventing unauthorized access to a host computer system." Ex. 1007, 1:3–5. Specifically, Kew describes a "method of preventing unauthorized access to a host computer system by a user at a remote terminal." *Id.* at 1:21–23. In Kew's method the host computer system accepts a user identification code input to the terminal by the user and generates a random code (Code A). *Id.* at 1:24–26. Using a transformation algorithm, Kew's computer system transforms Code A to transformed Code B. *Id.* at 1:27–30. The computer system also transmits Code A to user's receiver which transform's Code A to transformed Code C. *Id.* at 1:31–34. The user inputs Code C into the remote terminal and the computer system compares Code B with Code C, and if the Codes match permits access to the host computer system. *Id.* at 1:36–2:3.

d) Sormunen (Ex. 1008)

Sormunen is a Patent Cooperation Treaty application published August 28, 1998. Petitioner asserts that Sormunen is prior art under pre-AIA 35 U.S.C. § 102(a) and (b). Pet. 1.

Sormunen's "invention relates to 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. 1008, 1:3–5. Sormunen discloses the use of mobile communication systems including cellular systems, paging systems, and mobile phone systems. *Id.* at 4:36–5:1.

3. Ground 1: Alleged Obviousness of Independent Claim 5

Petitioner asserts that claim 5 is unpatentable over the combined teachings of Veneklase and Jonsson. Pet. 13. Petitioner addresses each limitation of claim 5 and provides the testimony of Dr. McNair in support of its position with respect to them claim 5. Pet. 17–46; Ex. 1003 ¶¶ 71–111. Patent Owner does not contest Petitioner's assertions for limitations [5.0]–[5.2] of claim 5. For the uncontested limitations ([5.0]–[5.2]), we have considered Petitioner's evidence and arguments with respect to these limitations, including the relevant testimony of Dr. McNair and find it to be sufficient to show that Petitioner has demonstrated a reasonable likelihood of prevailing in showing that Veneklase, either alone or in combination with Jonsson, teaches or suggests these limitations. Accordingly, we focus our discussion on contested limitations [5.3]–[5.6] and Patent Owner's arguments regarding these limitations.

a) Limitation [5.3]: 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;

Petitioner asserts that "*Veneklase* in combination with *Jonsson* teaches this limitation." Pet. 26 (citing Ex. 1003 ¶¶ 83–90). Regarding Veneklase, Petitioner asserts that Veneklase discloses assigning a password to the user; receiving the password by use of a first communication channel; generating a code in response to the received password; transmitting the code to the user via a second communications channel; transmitting the code to the computer; and allowing access to the computer only after the code is transmitted to the computer. Pet. 26 (citing Ex. 1005, 4:8–15).

Specifically, Petitioner asserts that "*Veneklase* discloses a user/password check module (i.e., a control module) located on the host computer system 402 (i.e., the computer processor)" and that the "user/password check module assigns two passwords, one that is known to the user and one that is not previously known to the user." Pet. 26–27 (citing Ex. 1005, Fig. 6).[8] Petitioner asserts further that "[w]hile *Veneklase* teaches an authentication system in which the user inputs both a token that is not known to the user beforehand (e.g., the random code) and a passcode that is known to the user (e.g., the received password), it does not disclose creating a new password based on those two items." *Id.* at 28.

Turning to Jonsson, Petitioner asserts that Jonsson discloses an authentication 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'" and that "[t]his challenge code generated by the system is a *token* because it is not known to the user before it is generated and sent to the user." Pet. 28 (citing Ex. 1006, 4:24–5:6; Ex. 1003 ¶¶ 86–87). Petitioner asserts further that "*Jonsson* discloses the use of a 'user input such as a personal identification number (PIN),' which by its very nature of being a user defined input, is known to the user beforehand" and that "*Jonsson* discloses an algorithm that '**calculates a response code [e.g., new password] based on the received challenge code [e.g., token], the user input (e.g., PIN) [e.g., passcode]**, and optionally [a] secret key.'" Pet. 29 (citing Ex. 1006, 3:3–10, 7:5–10, 8:12–14, 9:23–25).

---

[8] Here and for the remainder of this decision, we do not reproduce the colored font used in the Petition.

Petitioner asserts that it would have been obvious to combine Veneklase's token and passcode to "create a new password based on both of them." *Id.* at 28. Petitioner then asserts that "*Veneklase*'s authentication system would incorporate *Jonsson*'s teachings related to using an algorithm to create a new password (e.g., response code) based on a known passcode (e.g., the received password/PIN) and an unknown token (e.g., the random code/challenge code)." *Id.* at 30 (citing Ex. 1003 ¶¶ 83–89). Thus, according to Petitioner,

> *Veneklase* in combination with *Jonsson* teaches *a control module* (e.g., user/password check module) *executed on the computer processor configured to create a new password* (e.g., assigning a password to the user) *based at least upon a token* (e.g., random code) *and a passcode* (e.g., received password), *wherein the token is not known to the user* (e.g., generated by the system) *and wherein the passcode is known to the user* (e.g., received from the user), *the control module further configured to set a password associated with the user to be the new password* (e.g., set an expected response code).

Id. (citing Ex. 1003 ¶¶ 83–90).

In support of these assertions, Petitioner reasons that "[a] POSITA would have been motivated to make such a combination because having only the one password transmitted via the computer system is more efficient and secure." Pet. 31 (citing Ex. 1003 ¶ 91). According to Petitioner, "*Veneklase*'s system allows for authentication through user input of a known and unknown code at separate times in a two-step process, while a POSITA would look to *Jonsson* because it would provide the added benefit of reducing the steps to a single step and thus reducing the amount of time required for the authentication process." *Id.* Petitioner reasons further that "a POSITA would have been motivated to make such a combination because

implementing *Veneklase*'s authentication system with the algorithm of *Jonsson*'s system provides an additional layer of security." *Id.* at 31–32.

In addition, Petitioner asserts that Veneklase "explicitly discloses embodiments in which data streams are encoded and decoded using algorithms for additional security." Pet. 32 (citing Ex. 1005, 9:26–10:11; *KSR*, 550 U.S. at 418–419). Thus, according to Petitioner, "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, such as described in *Jonsson*, to provide additional security." *Id.* (citing Ex. 1003 ¶ 92). And, Petitioner asserts that "[a] POSITA would further be motivated to combine *Veneklase* and *Jonsson* because the combination merely uses a known technique to improve similar devices in the same way." *Id.* at 33 (citing *KSR* 550 U.S. at 401).

Patent Owner contends that "modifying *Veneklase's* system by abolishing the two-step authentication process, as proposed by Petitioner, would violate *Veneklase's* principle of operation." Prelim. Resp. 17. According to Patent Owner, "this two-step authentication process is a key feature of *Veneklase's* principle of operation, and a POSITA would not seek to remove steps as Petitioner proposes." *Id.* (citing Ex. 1005, 7:16–28). Patent Owner contends that "the proposed modification of *Veneklase* is far too drastic to be considered obvious, and thus the combination of *Veneklase* and *Jonsson* fails to render claim 5 obvious." *Id.* at 18 (citing MPEP § 2143.01(VI); *Plas-Pak Indus. v. Sulzer Mixpac AG*, 600 F. App'x. 755, 758 (Fed. Cir. 2015)).

We disagree with Patent Owner's arguments. Veneklase is directed to "a security and/or access restriction system . . .which is adapted to grant only

authorized users access to a computer system and/or to certain data which may be resident within the computer system and/or resident within a communications channel and/or other communications medium." Ex. 1005, 1:5–12. Patent Owner has not adequately demonstrated that the two-step authentication process is a key feature of Veneklase's principle of operation such that the proposed modification would render Veneklase's system inoperable. Rather, Patent Owner relies on unsupported attorney argument. *See* PO Resp. 17–18.

Incorporating Jonsson's teachings related to using an algorithm to create a new password would not destroy the principle of operation of Veneklase's security system because it only changes how Veneklase accomplishes its goal of preventing unauthorized access to a computer system, rather than defeating its goal of preventing such access. *See In re Mouttet*, 686 F. 3d 1322, 1332 (Fed. Cir. 2012). Further, we do not agree that *Plas-Pak* (a nonprecedential decision) supports the Patent Owner's contention that the proposed combination impermissibly changes Veneklase's principle of operation as Patent Owner has not identified differences between the two authentication processes that would be "unlikely to motivate a person of ordinary skill to pursue" the proposed combination. *Plas-Plak*, 600 F. App'x at 757-59.

Patent Owner contends that "Petitioner provides zero evidence that the security of its proposed combination is superior to the existing multi-layer/level security in *Veneklase*." Prelim. Resp. 19. Thus, according to Patent Owner, "there is no motivation to combine *Veneklase* and *Jonsson*." *Id.* at 20.

We disagree with Patent Owner's arguments. Petitioner does not propose modifying Veneklase to include Jonsson's teachings solely because the security of the proposed combination is superior to the security in Veneklase. Rather, Petitioner asserts that "[a] POSITA would have been motivated to make such a combination because having only the one password transmitted via the computer system is more *efficient* and secure." Pet. 31 (citing Ex. 1003 ¶ 91). The Petition explains how the combination is more efficient in that it requires only a single step which reduces the amount of time required for the authentication process. *Id.* Moreover, the Petition explains how the proposed combination is more secure than Veneklase's system in that it prevents unauthorized persons from accessing the computer system by engaging in SIM swapping. *Id.* at 32.

Patent Owner contends that the portion of Veneklase cited by Petitioner in support of its assertion that Veneklase provides explicit motivation for using Jonsson's algorithm in Veneklase's system "does not pertain to an algorithm." Prelim. Resp. 20 (citing Pet. 32 (citing Ex. 1005, 9:20–10:11)).

We disagree with Patent Owner's argument. Petitioner asserts that Veneklase "explicitly discloses embodiments in which data streams are encoded and decoded using algorithms for additional security." Pet. 32 (citing Ex. 1005, 9:26–10:11). The cited portion of Exhibit 1005 discloses, in relevant part, that

> System 70, as further shown, includes a data stream dividing means 74 which in one embodiment comprises a commercially available one input and two channel output time division or statistical multiplexor which samples the bits of received data and places, in a certain predetermined manner (e.g. alternately) some of the received data bits onto the first communications

> channel 76 and some of the received data bits onto the second communications channel 78. In this manner, one attempting to wrongfully intercept and/or access the data stream 72 would need access to both communications channels 76, 78 and would need to know the dividing *algorithm* that dividing means 74 utilizes to divide the received data for placement onto channels 76,78.

Ex. 1005, 9:33–48.

The cited portion further states, in relevant part, that

> security system 70 further includes a decoding means 88 which may comprise a commercially available microprocessor operating under stored algorithmic program control and which contains "mirror image" of the *algorithm* used to divide the data stream transmitted to it by means 74. In this manner, the data from each of the channels 76,78 is reconstituted onto single channel 89, in substantially the exact same manner that it was received by means 74.

Id. at 9:50–58.

b) Limitation [5.4]: a communication module configured to transmit the token to the personal communication device through the cell phone network;

Petitioner asserts that "*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.'" Pet. 35 (quoting Ex. 1005, 8:1–5). Petitioner asserts further that "the generated random number code and pager number are 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.'" *Id.* (citing Ex. 1005, 7:52–8:17, Fig. 6).[9]

Thus, according to Petitioner, "*Veneklase* 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)." Pet. 37 (citing Ex. 1003 ¶¶ 97–100). Petitioner asserts that "[a] POSITA would have understood that the 'conventional and commercially available communication channel 422' described in *Veneklase* is the same type of cell phone network disclosed in the '658 patent, which repeatedly makes clear that it covers both networks that communicate with cell phones and those that communicate with pagers." *Id.* at 36

Patent Owner agrees that "*Veneklase*'s system uses the received password (i.e., the first step in the two-step process) to lookup the user's phone number and transmit the randomly generated code to the user." Prelim. Resp. 22–23 (quoting Ex. 1005, 8:2–15; 6:10–37). Noting that "Petitioner's proposed combination includes replacing *Veneklase's* two-step authentication process (i.e., user transmission of *Veneklase's* password, and subsequent user transmission of *Veneklase's* random code) with the single step in *Jonsson* (i.e., user transmission of Jonsson's response code)," Patent Owner contends that "[t]he Petition is silent on how, following the proposed modification to *Veneklase* which abolishes user transmission of *Veneklase's* password, the user's phone number will be identified, and thus how the randomly generated code will be transmitted to the user's pager." *Id.*

[9] The Petition cites Ex. 1006. Veneklase, however, is Ex. 1005.

at 23–24. According to Patent Owner, "[w]ith *Veneklase's* modified system being unable to search the password list for a phone number, and thus unable to transmit the randomly generated code to the user's pager, *Veneklase's* modified system is inoperative," and thus, "there is no motivation for the proposed modification." *Id.* at 24.

We disagree with Patent Owner's characterization of the proposed modification as it pertains to limitation [5.4]. It is our understanding that in the proposed combination the user's device would be identified in accordance with Jonsson's teachings not Veneklase's. *See* Pet. 30–32. In other words, the user's device would be identified in response to the user's request for authentication as described in Jonsson. *See e.g.*, Ex. 1006, 9:2–8; 10:13–27, Fig. 3). Accordingly, the ability to look up the user's phone number is not a requirement of the combination and Patent Owner's argument is inapposite.

c) *Limitation [5.5]: 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,*

Petitioner asserts that "[i]n the combination with *Jonsson* discussed with respect to element [5.3], a POSITA would have understood that the new password . . . being sent back to computer 402 and compared against the expected value is the one created by the algorithm based on both the known passcode . . . and the randomly generated token." Pet. 38 (citing Ex. 1003 ¶¶ 83–89). Petitioner asserts further that "*Veneklase* discloses that [the] communication in which the user submits its credentials to the host computer and the initial sending of the random code to the personal device '**utilizes two distinct communication channels**.'" *Id.* at 39 (citing

Ex. 1005, 3:50–4:3, 7:11–28). Petitioner also asserts that a "POSITA would have understood that [Veneklase's] communication network is [a] *secure computer network* because the use of the authentication procedures described in *Veneklase* make secure the host computer system." *Id.* at 40 (citing Ex. 1005, 9:3–14; Ex. 1003 ¶¶ 101–104).

Patent Owner contends that Petitioner's assertions "conveniently glosses over the fact that the proposed combination requires modifying *Veneklase's* 'pager 420' to execute an algorithm that 'calculates a response code based on the received challenge code [and] the user input (e.g., PIN),' as performed by Jonsson's 'personal unit 20.'" Prelim. Resp. 26 (citing Ex. 1006, 8:12–14). Patent Owner further contends that "Petitioner presents zero evidence that *Veneklase's* 'pager 420' is capable of executing such an algorithm." *Id.*

We disagree with Patent Owner's arguments. Jonsson explicitly teaches that "the capacity for performing the necessary calculations exists in conventional cellular telephones and personal communication units [(i.e. pagers)], allowing the present invention to be implemented through software." Ex. 1006, 7:27–31. Thus, Jonsson's disclosure provides evidence that pagers, such as Veneklase's pager 420, are capable of executing Jonsson's algorithm.

In addition, Patent Owner contends that "Petitioner's proposed combination also fails to disclose 'an authentication module configured to receive the password from the user through a secure computer network.'" Pet. 27. As best understood, Patent Owner appears to be arguing that in Jonsson's system the password is not "received from the user" because it is not displayed to the user.

The claim language at issue, however, does not require that the password be known to the user. Rather, it requires that it be received from the user (in other words from the user's device). Thus, Patent Owner's argument is unconvincing.

> d) *Limitation [5.6]: 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.*

Petitioner asserts that Veneklase discloses that the user 404 sends a "'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**.'" Pet. 41 (citing Ex. 1005,[10] 6:45–7:10, 8:18–27). Petitioner asserts further that "*Veneklase* discloses an embodiment which 'includes a timer or "timing means" 40 which may comprise one or more software subroutines which are adapted to operate and/or execute within and/or upon computer 80,' such as a watchdog timer." *Id.* at 42 (citing Ex. 1005, 8:28–39).[11]

Petitioner asserts that in the combination with Jonsson "a POSITA would have understood that the new password (e.g., response code) being sent back to computer 402 and compared against the expected value is the one created by the algorithm based on both the known passcode (e.g., PIN)

[10] The Petition cites Ex. 1006; however, Veneklase is Ex. 1005.
[11] *See* note 5.

and the randomly generated token (e.g., challenge code)." Pet. 43 (citing Ex. 1003 ¶¶ 83–89). Thus, according to Petitioner, "the predetermined period would be the time between the receipt of the token (e.g., randomly generated challenge code) and the sending back of the newly created password (e.g., response code)." *Id.*

Turning to the deactivating part of limitation [5.6], Petitioner asserts that "*Veneklase*'s teaching is within the scope of the recited deactivating limitation because it is nearly identical to how this limitation is described in the '658 Patent." Pet. 43.

Patent Owner contends that "neither asserted reference discloses activating an account. And the Petition fails to argue, let alone show, that either reference discloses activating account access in response to generation of the new 'password,' which is 'based at least upon a token and a passcode.'" Prelim. Resp. 30–31 (citing Pet. 41–46). Patent Owner contends further that "[i]nstead, Petitioner incorrectly relies on steps in the prior art that occur well after the claimed 'password' is created." *Id.* at 31.

We disagree with Patent Owner's arguments. Claim 5 requires that the account be activated in response to the password. Ex. 1001, 12:41–43. It does not require that the account be activated in response to creation of the password. *Id.* On the record before us, Petitioner has adequately demonstrated that Veneklase discloses activation of the account in response to the password. *See* Pet. 41–42.

In addition, Patent Owner argues "that 'the predetermined period would be the time between receipt of the token (e.g., randomly generated challenge code) and the sending back of the newly created password (e.g., response code),'" and so, Petitioner's assertion "is flawed on its face because

the claimed 'predetermined amount of time' is the timeframe between activation and deactivation of the account." Prelim. Resp. 31 (citing Ex. 1001, 12:41–45).

We disagree with Patent Owner's argument. Claim 5 requires an authentication module that "deactivates the account within a predetermined amount of time after activating the account." Ex. 1001, 12:43–54). It does not require that the predetermined amount of time correspond to the entire time period between activation and deactivation of the account. On the record before us, Petitioner has adequately demonstrated that Veneklase discloses deactivation of the account within a predetermined amount of time. *See* Pet. 42–43.

e) Conclusion Regarding Ground 1

We have considered Petitioner's evidence and arguments with respect to all limitations of claim 5, including the relevant testimony of Dr. McNair and find it to be sufficient to show that Petitioner has demonstrated a reasonable likelihood of prevailing in showing that Veneklase and Jonsson, either alone or in combination, disclose each limitation of claim 5.

4. Ground 2: Alleged Obviousness of Claims 1 and 3–6

Having determined that Petitioner has demonstrated a reasonable likelihood of prevailing as to claim 5 on the basis of Ground 1, we do not address the patentability challenge on the basis of Ground 2.

III. CONCLUSION

For the foregoing reasons, we are persuaded that the Petition demonstrates a reasonable likelihood of prevailing in showing the unpatentability of at least one of the challenged claims of the '658 Patent. Because Petitioner has satisfied the threshold for institution as to at least one

claim, we institute *inter partes* review on all claims and all grounds raised in the Petition. *See SAS Institute Inc. v. Iancu*, 138 S. Ct. 1348, 1359–60 (2018) (holding that a decision to institute under 35 U.S.C. § 314 may not institute on fewer than all claims challenged in the petition).

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1 and 3–6 of the '658 Patent is instituted with respect to all grounds set forth in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of the '658 Patent shall commence on the entry date of this Order, and notice is hereby given of the institution of a trial.

FOR PETITIONER:

Jordan M. Rossen
Ashraf Fawzy
UNIFIED PATENTS, LLC
jordan@unifiedpatents.com
afawzy@unifiedpatents.com

For PATENT OWNER:

John Wittenzellner
Todd E. Landis
Michael J. Fagan, Jr.
Mark McCarthy
WILLIAMS SIMONS & LANDIS PLLC
johnw@wsltrial.com
tlandis@wsltrial.com
mfagan@wsltrial.com
mmccarthy@wsltrial.com