US 20070022301A1

(19) **United States**
(12) **Patent Application Publication**
Nicholson et al.
(10) **Pub. No.: US 2007/0022301 A1**
(43) **Pub. Date: Jan. 25, 2007**

(54) **SYSTEM AND METHOD FOR HIGHLY RELIABLE MULTI-FACTOR AUTHENTICATION**

(75) Inventors: **J. Joseph Nicholson**, New York, NY (US); **Paul Murphy**, Fort Lauderdale, FL (US); **Ivo Rothschild**, Westmount (CA)

Correspondence Address:
Paul D. Greeley
Ohlandt, Greeley, Ruggiero & Perle, L.L.P.
10th Floor
One Landmark Square
Stamford, CT 06901-2682 (US)

(73) Assignee: **Intelligent Voice Research, LLC**

(21) Appl. No.: **11/486,880**

(22) Filed: **Jul. 14, 2006**

Related U.S. Application Data

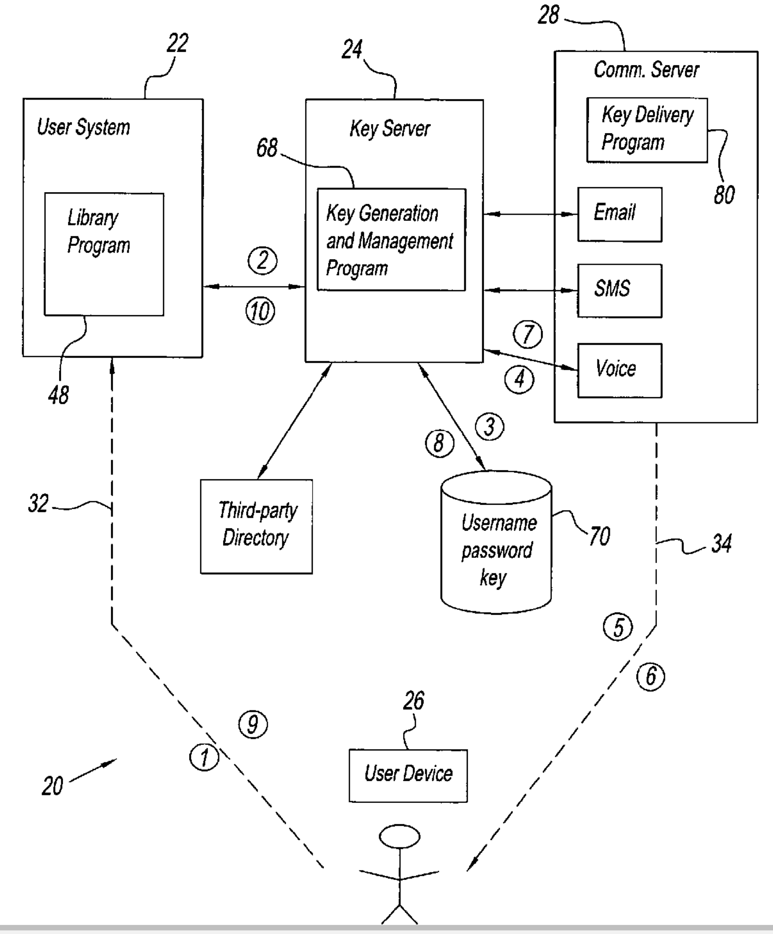
(60) Provisional application No. 60/700,506, filed on Jul. 19, 2005.

Publication Classification

(51) **Int. Cl.**
H04K 1/00 (2006.01)
(52) **U.S. Cl.** **713/184**

(57) **ABSTRACT**

A system and method for authenticating an online user by using different and independent communication services to enhance security. A key server validates the factors of authentication, namely a first factor (username/password) and a second factor (key). The key server generates and sends the key to the user with a different and independent communication service, e.g., telephone, SMS or email. The user then submits the key using the online communication service. A third factor, e.g., a second password or a biometric symbol of the user, can also be used. Validation of the biometric symbol can be a prerequisite to delivery of the key to the user. A plurality of the independent services can be daisy-chained.



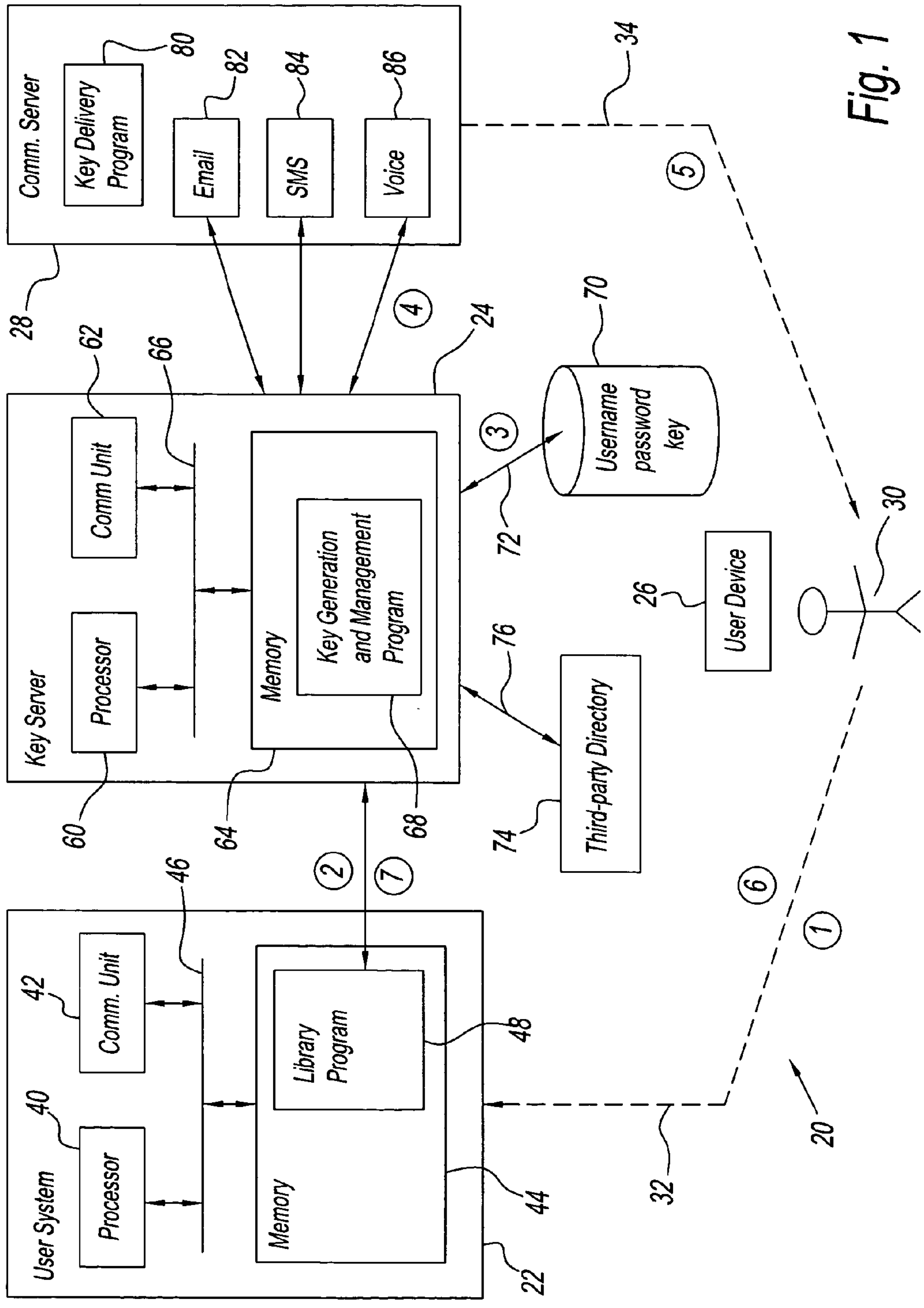

Comm. Server
Key Delivery Program
80
Email
82
SMS
84
Voice
86
34
28
5
4
24
62
66
70
Username password key
3
Key Server
Comm Unit
Processor
Memory
Key Generation and Management Program
72
30
26
User Device
76
Third-party Directory
60
64
68
74
2
7
6
1
46
User System
Comm. Unit
42
40
Processor
Memory
Library Program
48
44
22
32
20

Fig. 1

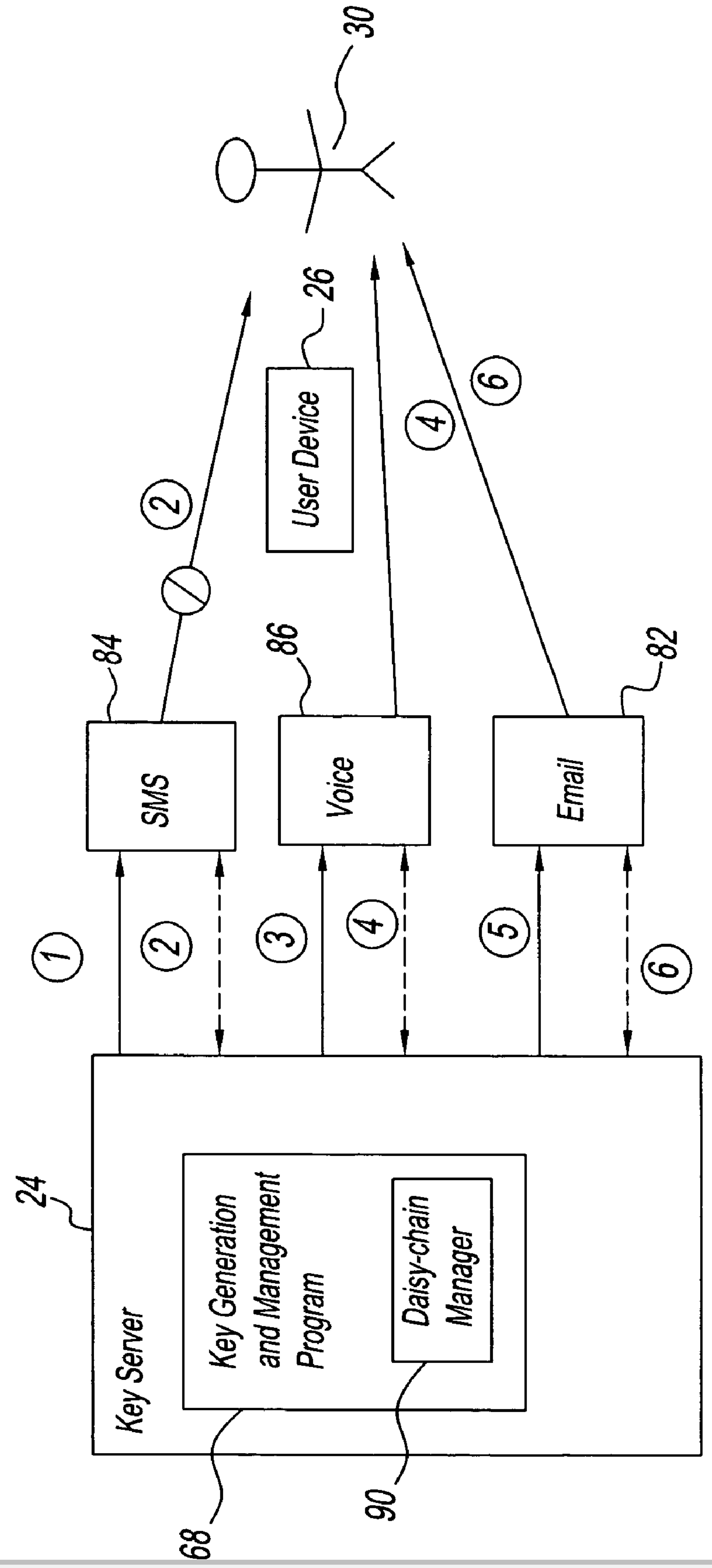

30
26
User Device
2
4
6
84
86
82
SMS
Voice
Email
1
2
3
4
5
6
24
Key Server
Key Generation and Management Program
Daisy-chain Manager
68
90

Fig. 2

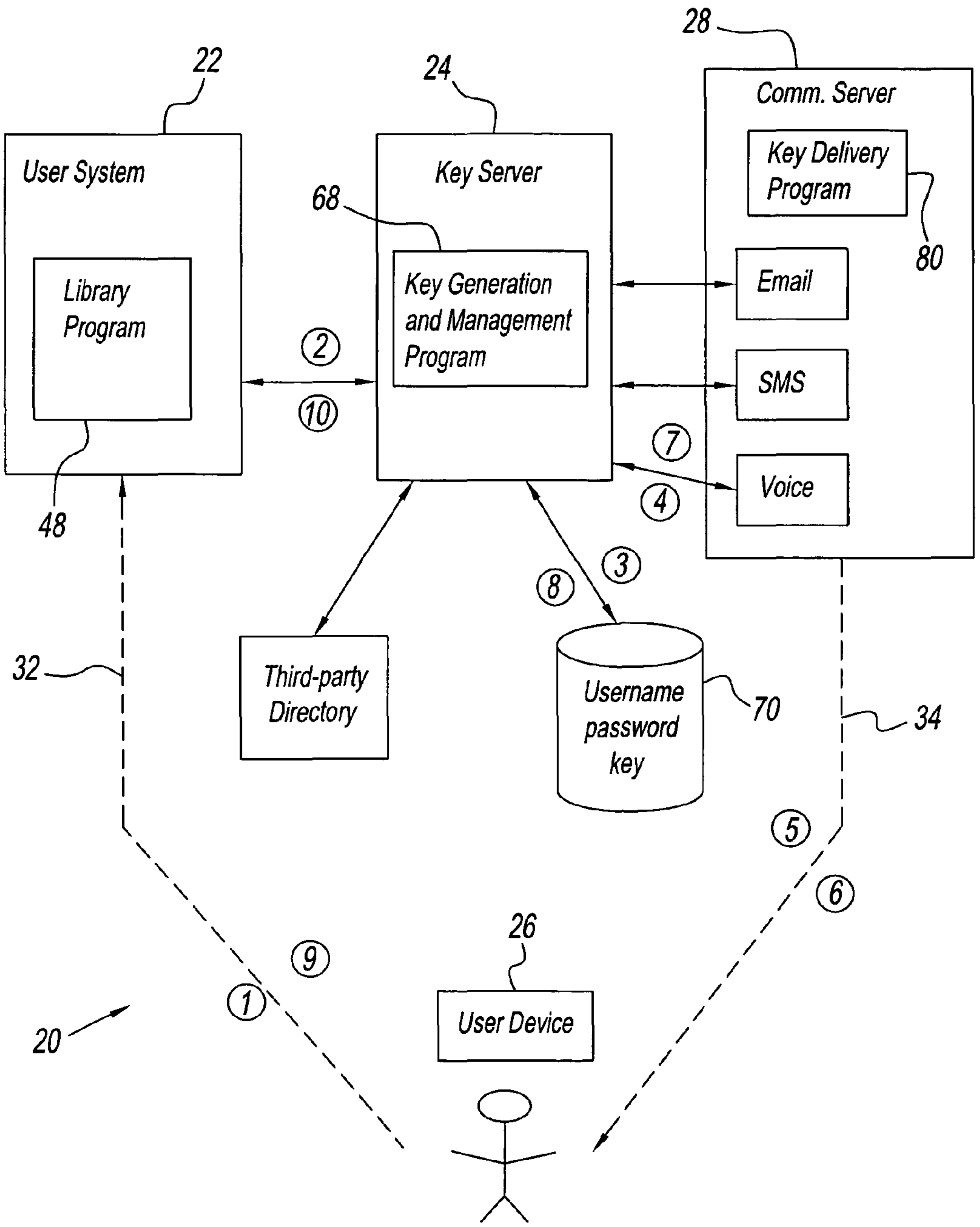

28
Comm. Server
Key Delivery Program
80
Email
SMS
Voice
22
User System
Library Program
48
24
Key Server
68
Key Generation and Management Program
2
10
7
4
3
8
Third-party Directory
Username password key
70
32
34
5
6
9
1
26
User Device
20

Fig. 3

SYSTEM AND METHOD FOR HIGHLY RELIABLE MULTI-FACTOR AUTHENTICATION

RELATED APPLICATION

[0001] This application claims the benefit of U.S. Provisional Patent Application, Ser. No. 60/700,506, filed Jul. 19, 2005, the entire contents of which are hereby incorporated by reference.

FIELD OF THE INVENTION

[0002] The present disclosure generally relates to multi-factor authentication of an on-line user and, in particular, to a system and method that employs two or more different and independent communication services.

BACKGROUND OF THE INVENTION

[0003] Multi-factor authentication is used to ensure that a person accessing a computer system is the person they claim to be by presenting multiple credentials of different types. Single-factor authentication requires the presentation of a datum known by the individual (e.g., a password, a user name or both). Two-factor authentication requires the additional presentation of something the user possesses (e.g., a key generated by a device).

[0004] For the sake of the present description, the term "fob" will mean any physical device capable of generating a one-time, expiring key. The fob could be a classic keychain, a card or software designed to execute on a particular mobile phone, etc. Two-factor authentication with fob-based keys for the second factor was initially used by only very secure computing facilities. Today it is used to protect many corporate networks against phishing, identity theft and other intrusive activities. In classic two-factor authentication, the first factor is something the user knows, e.g., a password or pass phrase. The second factor is something the user has, the fob-based key that generates and displays information synchronized with a central server, usually an alpha-numeric key that changes periodically. An IP provider has recently adopted two-factor authentication that gives users the option of using fobs to protect their accounts.

[0005] As the price of implementing multi-factor authentication decreases, it will be adopted by more and more of the institutions with which we interact on a daily basis. How long will it be before the average professional has to carry around a dozen fobs?

[0006] There is a need for authentication with high level security.

[0007] There is also a need to eliminate the use of fobs used to provide the second authentication factor.

SUMMARY OF THE INVENTION

[0008] A system of the present disclosure authenticates a user with a computer that receives a first factor and a third factor that are sent by the user using a first communication service and a second communication service, respectively. The computer comprises a program that generates a second factor, validates the first and third factors, then causes the second factor to be sent to the user using the second communication service and after receipt of the second factor sent by the user using the first communication service

[0009] In one embodiment of the system of the present disclosure, the first and third factors are different from one another.

[0010] In another embodiment of the system of the present disclosure, the first and third factors are selected from the group consisting of: password, pass phrase, username and any combination thereof.

[0011] In another embodiment of the system of the present disclosure, the third factor is a biometric symbol of the user. Preferably, the biometric symbol is selected from the group consisting of: a voiceprint, an iris scan, a fingerprint, a photograph or other symbol of a physical part of the user.

[0012] In another embodiment of the system of the present disclosure, the first communication service is an online service.

[0013] In another embodiment of the system of the present disclosure, the second communication service is selected from the group consisting of: SMS, telephone (land line or cellular) and page.

[0014] In another embodiment of the system of the present disclosure, the second factor comprises one or more series of alphabetic characters, numeric characters or both.

[0015] In another embodiment of the system of the present disclosure, the program validates the first and third factors by comparison with a repository of personal data of the user.

[0016] The method of the present disclosure authenticates a user by using a computer to perform the steps of:

[0017] receiving a first factor and a third factor that are sent by the user using a first communication service and a second communication service, respectively;

[0018] generating a second factor;

[0019] validating the first and third factors;

[0020] then causing the second factor to be sent to the user using the second communication service; and

[0021] after receipt of the second factor sent by the user using the first communication service, authenticating the user by validating the second factor.

[0022] In one embodiment of the method of the present disclosure the first and third factors are different from one another.

[0023] In another embodiment of the method of the present disclosure, the first and third factors are selected from the group consisting of: password, pass phrase, username and any combination thereof.

[0024] In another embodiment of the method of the present disclosure, the third factor is a biometric symbol of the user. Preferably, the biometric symbol is selected from the group consisting of: a voiceprint, an iris scan, a fingerprint, a photograph and other symbol of a physical part of the user.

[0025] In another embodiment of the method of the present disclosure, the first communication service is an online service.

[0026] In another embodiment of the method of the present disclosure, the second communication service is selected from the group consisting of: SMS, telephone (land

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.