Certification Under 37 C.F.R. § 1.8

I hereby certify that on November 17, 2011 this correspondence is being: (a) deposited with the United States Postal Service in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450; or (b) transmitted via facsimile to facsimile number 571-273-8300; or (c) electronically filed with the U.S. Patent Office.

Date: November 17, 2011 Signature: /Michael P. Fortkort/
Michael P. Fortkort (Reg. No. 35,141)

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

APPLICANT: NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI

SERIAL NO.: 12/210,926

FILING DATE: September 15, 2008

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

ATTORNEY DOCKET: KAMR002US0

CONFIRMATION NO.: 7516

VIA ELECTRONIC FILING SYSTEM
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

RESPONSE TO NON-FINAL OFFICE ACTION

Sir:

In response to the non-final Office Action mailed August 17, 2011, the Applicants hereby respectfully submit the following amendments and remarks:

Amendments to the Claims begin on page 2.

Remarks begin on page 16.

In the Claims:

Please amend the claims as follows:

1. (Currently Amended) A method for authenticating a user during an electronic transaction between the user and an External-Entity, the method comprising:

receiving electronically a request for a dynamic SecureCode for the user by a Central-Entity during the transaction between the user and the External-Entity;

generating during the transaction a dynamic SecureCode for the user in response to the request, wherein the dynamic SecureCode is valid for a predefined time and becomes invalid after being used;

providing said generated SecureCode to the user during the transaction;

receiving electronically by a Central-Entity a request for authenticating the user based on a digital identity during the transaction, which digital identity includes the SecureCode; and

authenticating by the Central-Entity the user during the transaction if the digital identity is valid.

2. (Original) A method as recited in claim 1, wherein said user has a pre-existing relationship with the External-Entity.

3. (Original) A method as recited in claim 1, wherein said user has no pre-existing relationship with the External-Entity.

4. (Previously Presented) A method as recited in claim 1, further comprising:

combining said generated SecureCode with a user-specific information using a predetermined algorithm to form a combined Secure-Code and user specific information;

maintaining the combined Secure-Code and user specific information at the Central-Entity;

using the predetermined algorithm to combine received user specific information received by the Central-Entity with a received SecureCode received by the Central-Entity to form a combined received SecureCode and received user specific information;

comparing the combined Secure-Code and user specific information with the combined received SecureCode and received user specific information to validate the user.

5-11. (Cancelled)

12. (Previously Presented) A method as recited in claim 1, wherein said External-Entity receives the user's digital identity.

13. (Previously Presented) A method as recited in claim 1, wherein said External-Entity submits a digital identity to the Central-Entity.

14. (Previously Presented) The method of claim 1, wherein said digital identity includes a user-specific information.

15. (Currently Amended) The method of claim 14, wherein the user specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an

identification phrase~~, wherein said identification phrase comprises one or more of the following: an account number, a telephone number, an IP address, a hardware key, a software key, a session ID, a token and a serial number~~.

16. (Original) The method of claim 1, wherein the transaction corresponds to a financial transaction.

17. (Original) The method of claim 1, wherein the transaction corresponds to a non-financial transaction.

18. (Previously Presented) The method of claim 1, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

19. (Previously Presented) The method of claim 1, wherein said transaction occurs over a communication network, wherein said communication network comprises one or more of the following: an Internet, a wireless network, a mobile network, a satellite network, and a private network.

20. (Previously Presented) The method of claim 1, wherein said transaction occurs over a communication network to which is coupled said user, said Central-Entity, and said External-Entity.

21. (Currently Amended) An apparatus for authenticating a user during an electronic

transaction with an External-Entity, the apparatus comprising:

a first Central-Entity computer adapted to:

generate a dynamic SecureCode for the user in response to a request during the transaction, wherein the dynamic SecureCode is valid for a predefined time and becomes invalid after being used; and

provide said SecureCode to the user;

a second Central-Entity computer adapted to validate a digital identity, which includes said SecureCode, and authenticate the user if the digital identity is valid.

22. (Previously Presented) The apparatus as recited in claim 21, wherein said user has a pre-existing relationship with the External-Entity.

23. (Previously Presented) The apparatus as recited in claim 21, wherein said user has no pre-existing relationship with the External-Entity.

24. (Previously Presented) The apparatus as recited in claim 21, wherein said External-Entity and said Central-Entity use a SecureCode that is algorithmically combined with said user-specific information.

25-31. (Cancelled)

32. (Previously Presented) The apparatus as recited in claim 21, wherein the user submits a digital identity to the External-Entity.

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.