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.: 11/333,400

FILING DATE: January 18, 2006

EXAMINER: Mr. Abdulhakim Nobahar

ART UNIT: 2432

TITLE: DIRECT AUTHENTICATION SYSTEM AND METHOD VIA TRUSTED AUTHENTICATORS

ATTORNEY DOCKET: KAMR001US0

CONFIRMATION NO.: 4456

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

RESPONSE TO NON-FINAL OFFICE ACTION

Sir:

The Applicant hereby petitions the Assistant Commissioner to grant a one (1) month extension of time, up to and including December 5, 2011, in which to file a response to the outstanding Office Action mailed August 5, 2011 ("Office Action") in the above-identified application. The small entity one-month extension fee in the amount of $75.00 may be charged

to the credit card on the attached credit card authorization form. Any additional fees may be charged to the deposit account of MICHAEL P FORTKORT PC, Deposit Account No. 50-3776.

In response to the non-final Office Action mailed August 5, 2011, the Applicants hereby respectfully submit the following amendments and remarks:

Amendments to the Claims begin on page 3.

Remarks begin on page 17.

In the Claims:

Please amend the claims as follows:

1-20. (Cancelled)

21. (Currently Amended) A computer implemented method to authenticate an individual in communication with an entity over a communication network during communication between the entity and the individual, the computer implemented method comprising:

receiving electronically a request for a dynamic code for the individual, which request is received during authentication of the individual by the entity;

calculating the dynamic code for the individual in response to the request during authentication of the individual by the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

sending electronically the dynamic code to the individual during authentication of the individual by the entity;

receiving electronically an authentication request to authenticate the individual based on a user information and the dynamic code included in the authentication request; and

verifying an identity of the individual based on the user information and the dynamic code included in the authentication request.

22. (Previously Presented) The computer implemented method of claim 21, wherein the request for the dynamic code is received by a computer associated with a first trusted-authenticator and the authentication request is received by the first trusted-authenticator.

23. (Previously Presented) The computer implemented method of claim 21, wherein the request for the dynamic code is received by a computer associated with a first trusted-authenticator and the authentication request is received by a computer associated with a second trusted-authenticator that is different than the first trusted-authenticator.

24. (Currently Amended) The computer implemented method of claim 21, wherein the dynamic code includes a ~~non-predictable and~~ time-dependent SecureCode.

25. (Previously Presented) The computer implemented method of claim 21, wherein at least the dynamic code is encrypted.

26. (Currently Amended) A computer implemented method for an entity to authenticate an individual over a communication network during communication with the individual, the method comprising:

requesting electronically both a user information and a dynamic code from the individual in order to validate the individual's identity during communication with the individual, which individual obtains the dynamic code from a computer associated with a trusted-authenticator during the communication between the individual and the entity, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

receiving electronically both the user information and the dynamic code from the individual; and

authenticating the individual based on verification by the trusted-authenticator of the user

information and the dynamic code received during communication between the individual and the entity

~~creating an authentication request message including both the user information and the received dynamic code and providing the authentication request message to a trusted-authenticator, the trusted-authenticator authenticating the individual based on a combination of the user information and the received dynamic code~~.

27. (Previously Presented) The computer implemented method of claim 26, wherein the user information and the dynamic code comprise credentials for verifying the individual's identity.

28. (Currently Amended) The computer implemented method of claim 26, wherein the dynamic code includes a ~~non-predictable and~~ time-dependent SecureCode.

29. (Previously Presented) The computer implemented method of claim 26, wherein at least the dynamic code is encrypted.

30. (Previously Presented) The computer implemented method of claim 26, wherein the entity corresponds to a business, organization, or another individual.

31. (Previously Presented) The computer implemented method of claim 26, wherein a computer associated with a first trusted-authenticator calculates the dynamic code and provides the dynamic code to the individual during communication between the individual and the 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.