Certification Under 37 C.F.R. § 1.8

I hereby certify that on March 1, 2012 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: March 1, 2012 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

AFFIDAVIT UNDER RULE 132

Applicants hereby submit this affidavit in support of their response to the Office Action mailed January 6, 2012 which rejected the pending claims.

This affidavit is being provided as testimony in the prosecution of U.S. Serial No. 12/210,926, and pursuant to the provisions of 37 C.F.R. § 1.132. The witness hereby avers and testifies as follows:

1. I am James Hewitt, residing at 12587 Fair Lakes Circle, #202, Fairfax, Virginia 22033.

2. I received a Bachelors of Arts in Philosophy from Vassar College in 1983.

3. I have been a Certified Information System Security Professional since 2001. My certification number is #21060 per ISC2.org.

4. From 1998-2002, I was Director of Professional Services at CertCo, Inc. in Cambridge, Massachusetts. During this time, I produced cryptographic systems used by Tier 1 banks for authentication of users, machines and financial transactions.

5. From 2002-2003, I was Secure Messaging Project Manager for the Commonwealth of Massachusetts Information Technology Division. During this period, I implemented a system for securing healthcare-related transactions statewide.

6. Since 2004 I have been Director of Security Governance for CGI Federal in Fairfax, Virginia. In this position, I design, implement and manage the security of large-scale applications for government and commercial clients.

7. I am familiar with the specification and pending claims of the present Application.

8. I have reviewed U.S. Patent Publication No. 2010/0100724 A1 by Kaliski, Jr. ("*Kaliski, Jr.*").

Nonce Not Equivalent to SecureCode

9. One of skill in the authentication art would understand that an **identifier** is non secret information such as a name or label that identifies an entity. And in the world of authentication an identifier is only used for identification of an entity and not for authentication of the entity.

10. One of skill in the authentication art would understand that in *Kaliski, Jr.*, a nonce is a **session identifier**. "The authentication server 730 returns the blinded result R to

the client 715, along with **a nonce or other session identifier** 772." *Kaliski, Jr.*, ¶ [0111] (emphasis supplied).

A *cryptographic nonce* is an arbitrary number used to establish the uniqueness or discreteness of an operation. That is, an operation such as a data request is accompanied by a nonce in order to demonstrate that the request is not a repeat or re-play of a previous request.

A *session* is a series of information exchanges between two communicating parties, usually involving an initiation protocol and more than one message in each direction.

In *Kaliski, Jr.* a nonce is used for identification of a user's session. In the client/server world, a session refers to all the requests that a single client makes to a server. A session is specific to each user and for each user a new session is created to track all the requests from that user. Every user has a separate session and separate session identifier is associated with that session.

11. One of skill in the authentication art would understand that the nonce in *Kaliski, Jr.* is not equivalent to the SecureCode of the present application. A nonce is a session identifier associated with a user's session, but a nonce is not used for authentication of a user, as is the SecureCode recited in the claims of *Kamrani*.

12. One of skill in the authentication art would understand that the statement "the nonce corresponds to the recited dynamic SecureCode" is inaccurate. In *Kaliski, Jr.* the web server receives the nonce and hardened password from the client and authenticates the user based on successful decryption of a digital signature associated with the hardened password. *Kaliski, Jr., ¶¶ [0109] and [0112].* The nonce is used by the web server to identify the user and the hardened password used in the authentication process of authenticating the user. In *Kamrani*, a dynamic code authenticates a user whereas in *Kaliski, Jr.* a nonce is a session identifier. Therefore the argument that "the nonce corresponds to the recited dynamic code" is invalid.

No Authentication Request Message

13. One of skill in the authentication art would understand that in the system of *Kaliski, Jr.* there is nothing equivalent to a Central Entity receiving an authentication request message, as recited in the claims at issue. The Office Action equates the claimed authentication request message to message 776 of *Kaliski, Jr.* But, message 776 that the authentication server in FIG 7 of *Kaliski, Jr.* receives is NOT an authentication request message. Rather, message 776 indicates simply whether or not the authentication of the client by the web server was successful. *See Kaliski, Jr.* ¶¶ *[0109] through [0112]*. This message 776 is a one way acknowledgement and expects no return, whereas the authentication request message as recited in the claims at issue is a different type of message than the cited acknowledgement as the claimed authentication request should generate a response because it is a REQUEST as opposed to an acknowledgement. Thus, the message in *Kaliski, Jr.* cited by the Office Action at issue is not equivalent to the claimed authentication request message in *Kamrani*. Thus, one of skill in the authentication art would understand that the argument in the Office Action equating the claimed authentication request message to the acknowledgement message 776 in *Kaliski, Jr.* is not valid.

No Central Entity Authenticating User

14. One of skill in the authentication art would understand that there is nothing in *Kaliski, Jr.* equivalent to a Central Entity authenticating the user as recited in the claims at issue. The Office Action equates the Central Entity to the authentication server 730 in *Kaliski, Jr.* But, the authentication server 730 in FIG 7 never authenticates the client. Rather, the web server 710 authenticates the client based on successful decryption of the client's digital signature associated with the hardened password. *See Kaliski, Jr.* ¶¶ [0109] through [0112]. Moreover, the web server 710 of *Kaliski, Jr.* does not generate anything

equivalent to the claimed SecureCode, as recited in the claims at issue. Thus, neither the web server 710 nor the authentication server 730 of *Kaliski, Jr.* performs the functions of the Central Entity recited in the claims.

15. One of skill in the authentication art would understand that in *Kaliski, Jr.* a user's client application generates a hardened password (based on the blinded result R received from the authentication server) and submits the generated hardened password to the web server and not to the authentication server cited by the Office Action. In *Kaliski, Jr.* the client receives the blinded result R along with a nonce from the authentication server and generates the hardened password at the client side for authentication to the web server. *Kaliski, Jr.*, ¶ [0111].

16. One of skill in the authentication art would understand that the argument in the Office Action equating the claimed "authenticating by the Central-Entity the user during the transaction, if the digital identity is valid" with the authentication protocol in *Kaliski, Jr.* is not valid. The authentication server 730 does not authenticate the client; it is the web server that authenticates the client. And, the web server 710 of *Kaliski, Jr.* also cannot be the claimed Central Entity because the web server does not generate anything equivalent to the claimed SecureCode. Thus, there is no Central Entity authenticating the user in *Kaliski, Jr.*

Authentication Process Different

17. The web server of *Kaliski, Jr.*stores the user's personal information as encryption secrets (See *Kaliski, Jr., ¶ [0103]*) and the encrypted secrets are stored such that they can be decrypted with a decryption key/hardened password. In *Kaliski, Jr.* a blind function evaluation protocol is used by the client to drive a decryption key/hardened password from a blinded result R received from the authentication server (See *Kaliski, Jr., ¶ [0111]*), to decrypt the encrypted secrets. The web server authenticates the client if the hardened password received from the client successfully decrypt user's information.

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**