I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: December 17, 2012
Electronic Signature for Matthew H. Grady: /Matthew H. Grady/

Docket No.: W0537-701320
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 13/237,184 Confirmation No.: 7352

Filed: September 20, 2011 Art Unit: 3621

For: UNIVERSAL SECURE REGISTRY Examiner: C. K. Cheung

AMENDMENT IN RESPONSE TO NON-FINAL OFFICE ACTION UNDER 37 C.F.R. 1.111

Commissioner for Patents
Alexandria, VA 22313-1450

Dear Madam:

INTRODUCTORY COMMENTS

In response to the Office Action dated August 15, 2012, please amend the above-identified U.S. patent application as follows:

Amendments to the Specification begin on page 2 of this paper.

Amendments to the Claims are reflected in the listing of claims which begins on page 3 of this paper.

Remarks/Arguments begin on page 9 of this paper.

AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph beginning at page 1, line 4 with the following:

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims the benefit under 35 U.S.C. § 120 as a continuation of U.S. patent application No. 12/393,586 filed February 26, 2009, now U.S. Patent No. 8,234,220 which is a continuation-in-part of each of U.S. patent application serial no. 11/760,732 filed June 8, 2007, now U.S. Patent No. 7,809,651; U.S. patent application serial no. 11/760,729 filed June 8, 2007, now U.S. Patent No. 7,805,372; and U.S. patent application serial no. 11/677,490 filed February 21, 2007, now U.S. Patent No. 8,001,055. This application also claims the benefit under 35 U.S.C. § 120 as a continuation-in-part of U.S. patent application no. 13/168,556 filed on June 24, 2011, which claims the benefit under 35 U.S.C. § 120 as a continuation of U.S. application no. 11/677,490. Each of U.S. application nos. 11/760,732, 11/760,729 and 11/677,490 claim priority under 35 U.S.C. § 119 (e) to U.S. Provisional Application Nos. 60/812,279 filed on June 9, 2006, and 60/859,235 filed on November 15, 2006. U.S. application no. 11/677,490 also claims priority under 35 U.S.C. § 119 (e) to U.S. Provisional Application No. 60/775,046 filed on February 21, 2006. Each of the above-identified applications is hereby incorporated herein by reference in its entirety.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) An electronic ID device configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction, comprising:

a biometric sensor configured to receive a biometric input provided by the user;

a user interface configured to receive a user input including secret information known to the user and identifying information concerning an account selected by the user from the plurality of accounts;

a communication interface ~~link~~ configured to communicate with a secure registry; and

a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface and the communication interface ~~link~~, the processor being programmed to activate the electronic ID device based on successful authentication by the electronic ID device of at least one of the biometric input and the secret information, the processor also being programmed such that once the electronic ID device is activated the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, ~~the identifying information, and at least one of~~ information derived from at least a portion of the biometric input, and the secret information, and to communicate the encrypted authentication information via the communication interface ~~link~~ to the secure registry.

2. (Currently Amended) The device of claim 1, wherein the communication interface ~~link~~ is configured to wirelessly transmit the encrypted authentication information to a point-of-sale (POS) device, and wherein the secure registry ~~POS device~~ is configured to receive ~~transmit~~ at least a portion of the encrypted authentication information from the POS device ~~to the secure registry~~.

3. (Cancelled)

4. (Currently Amended)The device of claim 2, wherein the device comprises ~~the processor is configured to generate the encrypted authentication information from each of the non-predictable value, the identifying information, the information concerning the biometric input and the secret information~~ a discrete code associated with the electronic ID device.

5. (Currently Amended) The device of claim 1, wherein at least a portion of the biometric received by the biometric sensor is communicated to the secure registry for authentication prior to generation of the encrypted authentication information.

6. (Original) The device of claim 1, wherein the secret information includes the identifying information.

7. (Original) The device of claim 1, further comprising a memory coupled to the processor, wherein the memory stores information employed by the device to authenticate the biometric received by the biometric sensor.

8. (Original) The device of claim 7, wherein the device does not permit the entry of the user input if the biometric input received by the biometric sensor is determined to not belong to an authorized user of the device.

9. (Currently Amended) The device of claim 8, wherein the secret information known to the user includes a PIN, and wherein the authentication of both the secret information and the biometric input activate the device for ~~the~~ a financial transaction.

10. (Original) The device of claim 9, further comprising a memory coupled to the processor, wherein data stored in the memory is unavailable to an individual in possession of the device until the device is activated.

11. (Original) The device of claim 10, wherein the data is subject to a mathematical operation that acts to modify the data such that it is unintelligible until the device is activated.

12. (Currently Amended) The device of claim 9, further comprising a memory coupled to the processor and configured to store an electronic serial number of the device, wherein the processor is configured to generate a seed using at least two of the electronic serial number, a discrete code associated with the device, the PIN, a time value, and the biometric input to generate the encrypted authentication information, and wherein the seed is employed by the processor to generate the non-predictable value.

13. (Currently Amended) The device of claim 1, wherein the biometric sensor is configured to receive and process at least one of a fingerprint, a speech/voice input, an iris scan, a retina scan, a facial scan, ~~a fingerprint~~, written information and a DNA input.

14. (Currently Amended) The device of claim 13, ~~further comprising~~ wherein the processor is configured to generate account identifying information for the respective one of the plurality of accounts, wherein the account identifying information does not identify an account number of the respective one of the plurality of accounts ~~a handheld device including each of the biometric sensor, the user interface, the communication link and the processor~~.

15. (Currently Amended) A method of generating authentication information comprising acts of:

authenticating an identity of a user to an electronic ID device based on at least one of biometric data received by the device from the user and secret information known to the user and provided to the device;

activating the electronic ID device based on successful authentication;

generating, responsive to activating, a non-predictable value with the device;

receiving, in a user interface, identifying information from the user concerning a selected one of a plurality of user accounts; ~~and~~

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.