

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: July 15, 2016
Electronic Signature for John N. Anastasi: /John N. Anastasi/

Docket No.: W0537-700924
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 15/019,660

Confirmation No.: 1202

Filed: February 9, 2016

Art Unit: 3668

For: METHOD AND APPARATUS FOR SECURE
ACCESS PAYMENT AND IDENTIFICATION

Examiner: C. K. Cheung

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

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

INTRODUCTORY COMMENTS

In response to the Office Action dated April 15, 2016, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 6 of this paper.

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) A system for authenticating a user for enabling a transaction, the system comprising:

a first device including:

a first processor, the first processor programmed to authenticate a user of the first device based on secret information and to retrieve or receive first biometric information of the user of the first handheld device; and

a first wireless transceiver coupled to the first processor and programmed to transmit a first wireless signal including first authentication information of the user of the first handheld device;

a biometric sensor configured to capture the first biometric information of the user; and

wherein the first processor is programmed to generate one or more signals including the first authentication information, an indicator of biometric authentication, and a time varying value in response to valid authentication of the first biometric information, and to provide the one or more signals including the first authentication information for processing by transmitting to a second device; and

wherein the first processor is further configured to receive an enablement signal from the second device;

the system further including the second device that is configured to provide the enablement signal indicating that the second device ~~an approved~~ the transaction ~~from the second device,~~ wherein the enablement signal is provided from the second device based on use of the one or more signals[.];

wherein the second device includes a second processor that is configured to ~~retrieve biometric information associated with the user of the first handheld device from stored biometric information of a plurality of first users stored in a second memory of the second device, or receive proof of~~ provide the enablement signal based on the indication of biometric authentication associated with of the user of the first handheld device, and wherein the second

~~processor is also configured to use at least a portion of the first authentication information, and second authentication information of the user of the first handheld device with the proof of biometric authentication to enable and complete processing of the transaction, wherein processing of the transaction includes authentication of an identity of the user of the first handheld device to enable the transaction.~~

2. (Currently Amended) The system according to claim 1, wherein the first processor is programmed to determine the first authentication information so that the first authentication information is generated based on[,] at least part of the first biometric information or generated based on receiving the first biometric information.

3. (Currently Amended) The system according to claim 1, ~~wherein the first handheld device is configured to communicate with a second device, the second device~~ including:
~~a second processor;~~
a second communication interface coupled to the second processor, and
wherein the second processor is configured to[:] receive the first authentication information of the user of the first handheld device[;], to retrieve or receive the authentication information of the user of the first handheld device; and use the first authentication information and the second authentication information to authenticate the user of the first handheld device to enable the transaction.

4. (Currently Amended) The system according to claim 1, ~~wherein the first handheld device is configured to communicate with a second device, the second device~~ including:
~~a second processor;~~
a second wireless transceiver coupled to the second processor, and
wherein the second processor is configured to[:] receive the first authentication information of the user of the first handheld device[;], to retrieve or receive the second authentication information of the user of the first handheld device; and use the first authentication information and the second authentication information to authenticate the user of the first handheld device ~~with the second device~~ to enable the transaction.

5. (Original) The system of claim 1, wherein the first processor is further configured to compare stored authentication information with the authentication information of the user and configured to enable the first device based on a valid comparison.

6. (Currently Amended) The system of claim 1, wherein the first processor is further configured to encrypt the first authentication information to communicate to [a] the second device.

7. (Currently Amended) The system of claim 1, wherein the first handheld device includes a first memory coupled to the first processor ~~included in the first handheld device~~ and configured to store ~~respective~~ the first biometric information.

8. (Original) The system of claim 1, wherein the first authentication information includes a multidigit public ID code for a credit card account, which a credit card issuer can map to a usable credit card number.

9. (Original) The system of claim 1, wherein the first processor is further configured to communicate information associated with the biometric information of the user of the first device.

10. (Currently Amended) The system of claim 1, further comprising:
wherein the first handheld device includes a user interface coupled to the first processor ~~included in the first handheld device;~~
wherein the first processor is configured to receive the first biometric information of the user of the first device[,]; and
wherein the biometric information is employed by the user of the first handheld device to initiate payment for the transaction.

11. (Currently Amended) The system of claim 1, wherein the first device is configured to communicate with the second device that is a networked credit card validation-information entity configured to approve or deny financial transactions based on authentication of the user.

12. (Currently Amended) A system for authenticating a user for enabling a transaction, the system comprising:

a first device including:

a biometric sensor configured to capture a first biometric information of the user;

a first processor programmed to: 1) authenticate a user of the first device based on secret information, 2) retrieve or receive first biometric information of the user of the first handheld device, 3) authenticate the user of the first device based on the first biometric, and 4) generate one or more signals including first authentication information, an indicator of biometric authentication of the user of the first handheld device, and a time varying value[,]; and

~~wherein generating occurs responsive to valid authentication of the first biometric;~~

a first wireless transceiver coupled to the first processor and programmed to wirelessly transmit the one or more signals to a second device for processing;

wherein generating the one or more signals occurs responsive to valid authentication of the first biometric information; and

wherein the first processor is further programmed to receive an enablement signal indicating an approved transaction from the second device, wherein the enablement signal is provided from the second device based on acceptance of the indicator of biometric authentication and use of the first authentication information and use of second authentication information to enable the transaction.

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.