

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
29 March 2001 (29.03.2001)

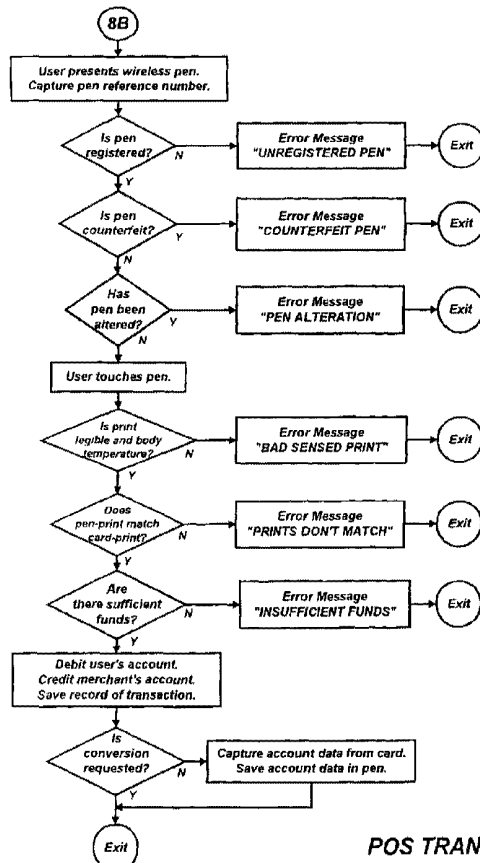
PCT

(10) International Publication Number  
WO 01/22351 A1

- (51) International Patent Classification<sup>7</sup>: G06K 9/00, (71) Applicant and  
H04M 11/00, G06F 9/06, H04L 9/00 (72) Inventor: BLACK, Gerald, R. [US/US]; 30590 South-  
field Road, Suite 160, Southfield, MI 48076 (US).
  - (21) International Application Number: PCT/US00/19652
  - (22) International Filing Date: 18 July 2000 (18.07.2000) (81) Designated States (national): AE, AG, AL, AM, AT, AU,  
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ,  
DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR,  
HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR,  
LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ,  
NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM,  
TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
  - (25) Filing Language: English
  - (26) Publication Language: English
  - (30) Priority Data: (84) Designated States (regional): ARIPO patent (GH, GM,  
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian  
patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European  
patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,  
IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG,  
CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
- |            |                                |    |  |
|------------|--------------------------------|----|--|
| 60/154,590 | 17 September 1999 (17.09.1999) | US |  |
| 60/163,433 | 3 November 1999 (03.11.1999)   | US |  |
| 60/177,390 | 20 January 2000 (20.01.2000)   | US |  |
| 09/490,687 | 24 January 2000 (24.01.2000)   | US |  |
| 09/535,411 | 24 March 2000 (24.03.2000)     | US |  |
| 60/207,892 | 25 May 2000 (25.05.2000)       | US |  |

[Continued on next page]

(54) Title: IDENTITY AUTHENTICATION SYSTEM AND METHOD



(57) Abstract: The identity authentication system (Figure 8) employs biometric technology to ensure the integrity of electronic transactions and networks. Positioned at the center of the system is a wireless device (15), which includes a biometric sensor (20) that captures one or more biometric properties when touched. When fingerprint sensors are used, the sensors are positioned in the stylus grip (30), one sensor for the index finger, and a second sensor for the thumb. In one variation, one-to-one biometric matching is used. Each participant carries a wireless device that includes an encrypted biometric for reference purposes to gain access into the system. Processing is simplified since the system needs only to make a "MATCH" or "NO MATCH" decision. In a second variation that is particularly useful in controlled environments, one-to-many biometric matching is used. During each event access request, the community of the reference prints is searched for a match with the applicant. Each member of the community needs to carry nothing on one's person to participate in the system. In either variation, the stylus is either attached to each site or is portable, one such stylus being carried by each participant.

POS TRANSACTION  
W/ PEN-CONVERSION



WO 01/22351 A1



**Published:**

- *With international search report.*
- *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

## IDENTITY AUTHENTICATION SYSTEM AND METHOD

This Application is related to and claims priority under U.S. Provisional Application No. 60/207,892 entitled "Identity Authentication System and Method" filed on May 25, 2000, U.S. Provisional Application No. 09/535,411 entitled "Method for Identity Authentication" filed on March 24, 2000, U.S. Serial No 09/490, 687 entitled "Writing Implement For Identity Authentication System" Filed 20 January 2000, U.S. Provisional Application No. 60/177,390 entitled "Writing Implement For Identity Authentication System" filed 20 January 2000, U.S. Provisional Application No. 60/163,433, entitled "Writing Implement For Identity Authentication System" filed 11 November 1999, U.S. Provisional Application No. 60/154,590 entitled "Writing Implement for Identification Authentication System" filed 17 September 1999, U.S. Provisional Application No. 60/144,028 entitled "Biometric Pen And Encryption Device" filed 16 July 1999.

### FIELD OF THE INVENTION

The invention relates generally to a method for authenticating the identification of a person using biometric means, and more particularly, for use at point-of-sale terminals, for use in various closed environments, for accessing a computer network, for applications involving pen-based computers and smart-pens, and for e-commerce.

### BACKGROUND OF THE INVENTION

Wireless (e.g., radio, infrared, microwave) communication links now enable computer systems comprised of handheld computers that have the capability of being networked at all times and in all locations. These handheld computers represent is the strongest trend in the computer industry, and wireless communication is one of the strongest trends in the telecommunication

industry. Also, in palm and pocket computers the input device is a pen' and the screen is the paper. The learning curve is minimal compared to a laptop. This is significant for non-computer users who otherwise would have to concentrate more on learning how to use the laptop than doing their jobs.

The global workforce is increasingly mobile and pen-based computing is on the rise. Smart handheld devices are emerging from the realm of individual purchases to enterprise deployment, as they become key tools for connectivity to the corporate environment. Development of handheld applications and wireless technology tailored for the enterprise represent are serving the increasing the remote and mobile worker population.

Widespread acceptance of biometrics means use in areas that daily affect the lives of millions of people. By replacing PIN's, biometric techniques prevent the unauthorized access to or fraudulent use of ATMs, cellular phones, smart cards, desktop PC's, workstations, and computer networks, For financial transactions conducted via telephone and wire, biometrics can replace PIN's and passwords. In buildings and work areas, biometric techniques replace keys, badges, and readers.

An example of a rapidly growing biometric technology, fingerprints offer an infallible means of personal identification and are rich in information content. The use of fingerprints for identification dates back many decades, but gained wide acceptance about 100 years ago. Fingerprints are the biometric that form the basis of all worldwide identification. Fingerprints don't change with time while other physical characteristics do. Fingerprint minutiae uniquely identify fingerprints. It has been proven that minutiae, were unchanging and repeatable features of each fingerprint, and were individually unique. Each finger has a unique arrangement of ridge detail. There are two major types of information in a fingerprint. First is the ridge flow information, and second is the specific features or minutiae (minutia) of the fingerprint. As used herein, the term

'minutia is used to denote both the singular and plural. Fingerprints uniquely identify an individual based on their information content. Information is represented in a fingerprint by the minutia and their relative topological relationships. The number of minutiae in a fingerprint varies from one finger to another, but, on average, there is between eighty (80) and one-hundred-and-fifty (150) points of minutia per fingerprint. In the fingerprint context, a large store of fingerprints exists in law enforcement offices around the country. Since fingerprints never change, a person need only be fingerprinted once to be in the system.

U.S. Patent No. 5,680,470 (Moussa et al.) discloses a method of signature authentication involving a set of template signatures that are examined for test features, which are normalized, and irrelevant features are removed. Similarly, U.S. Patent No. 5,559,895 (Lee et al.) discloses a system for real time signature authentication where the signatures are digitized for statistical analysis and various personal features are selected.

Current stylus-type authentication systems use metric-type sensors - accelerometers and pressure sensors to measure stylus pressure and stroke sweep in the users' signature. U.S Patent No. 5,774,571 (Marshall) discloses a stylus with multiple sensors for biometric authentication including grip pressure sensors and gyroscopes. U.S. Patent No. 4,513,437 (Chainer et al.) discloses another data input stylus for signature authentication, which includes accelerometers and pressure sensors. U.S. Patent No. 5, 247,137 (Epperson) discloses a stylus that enables biometric identification by means of comparison of graphics data and textural data from a remote location. The stylus also captures strokes and gestures, which can also be used for confirming identification. U.S. Patent 5,103,486 (Grippi) discloses a system for using a combination of biometrics at POS terminals. Prisms are used to capture the fingerprint of the index finger while the individual signs his/her name. The fingerprint image and the signature are processed to form a composite

# 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.