PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00, H04Q 1/00

A1

(11) International Publication Number: **WO 99/56429**

(43) International Publication Date: 4 November 1999 (04.11.99)

(21) International Application Number: PCT/US99/08990

(22) International Filing Date: 26 April 1999 (26.04.99)

(30) Priority Data:

09/066,643	24 April 1998 (24.04.98)	US
09/298,326	23 April 1999 (23.04.99)	US

(71) Applicant: IDENTIX INCORPORATED [US/US]; 510 North Pastoria Avenue, Sunnyvale, CA 94086 (US).

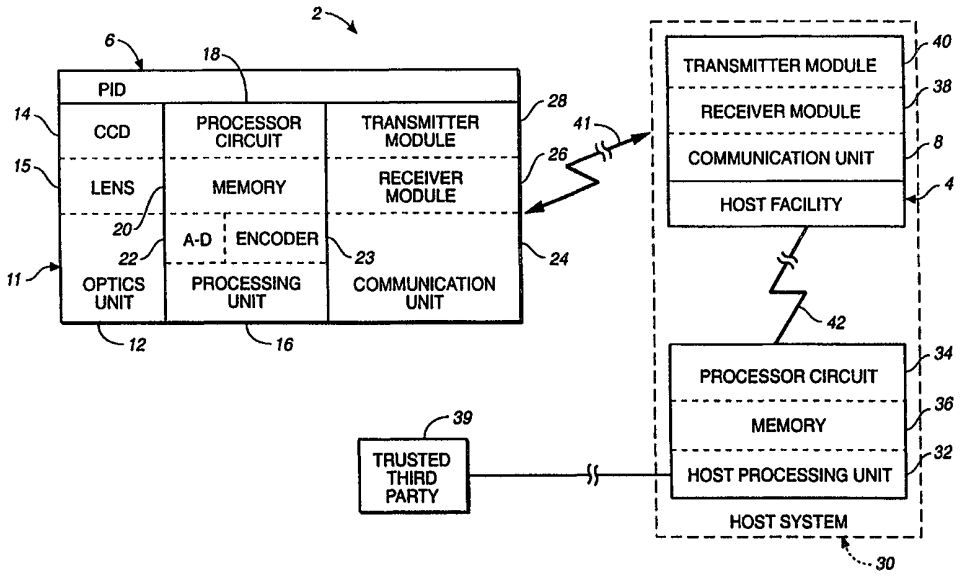
(72) Inventors: SCOTT, John, D.; 9 Pine Valley Road, Galson, NSW 2159 (AU). CURTIS, Terence, P.; 10 Selina Avenue, Kariong, NSW 2250 (AU).

(74) Agent: GARCIA, Edouard, A.; Fish & Richardson P.C., Suite 100, 2200 Sand Hill Road, Menlo Park, CA 94025 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, 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, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, 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).

Published
With international search report.

(54) Title: PERSONAL IDENTIFICATION SYSTEM AND METHOD



(57) Abstract

A portable, hand–held personal identification device (6) and method for providing secure access to a host facility (4) includes a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative of the sensed biometric trait. A processing unit responsive to the biometric signal is adapted to compare the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is unique to the enrolled person, and to provide a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person. The verification signal (41) includes information indicative of the enrolled person or the device. A communication unit, including a transmitting circuit (28), is adapted to transmit the verification signal to a host system (30).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

PERSONAL IDENTIFICATION SYSTEM AND METHOD

Background of the Invention

The invention relates to a personal identification system and method for allowing access to secure facilities.

Some security systems, such as home security systems and door locks, require a user to enter a fixed code into a device at a host facility before allowing a person access to the facility. Other systems, such as automated teller machines (ATM), require a person to submit an authorized card and also to enter a fixed code that is associated with the person's bank accounts. Automobile alarms, locks, and disabling devices, and garage door openers can be operated by pressing a button on a small remote device to transmit a coded signal to a receiving unit on the automobile or garage.

Each of these security systems can be operated by any person who is in possession of the fixed code, the card or the transmitting device, as the case may be. Therefore, each of these systems is inherently insecure. Where absolute security is essential, some host facilities employ a biometric sensor to measure a biometric trait of a person requesting access to the host facility. The biometric trait is a unique identifier of a person, and can be, for example, a person's fingerprint, voice pattern, iris pattern, or the like. The requesting person also enters other identifying information about himself. The measured biometric trait is compared with stored biometric data associated with the identified person and, if there is a match, the requesting person is allowed entry or access to the host facility.

In presently available biometric systems, each authorized person registers with the host facility by providing a sample of their biometric trait, for example, by having his fingerprint optically scanned into a host system data base. Each host facility must have a biometric sensor, access to the database of registered persons' biometric trait registration data, and a processing system capable of quickly searching the database and conducting the comparison to verify a person's identity. However, if the set of authorized persons is large, such a system would require a huge database to store the fingerprint images of all the authorized persons, and the

identification process would become slower as the set of authorized persons increases.

Summary of the Invention

According to one aspect of the invention, a portable personal identification device for providing secure access to a host facility includes a biometric sensor system capable of sensing a biometric trait of a user that is unique to the user and providing a biometric signal indicative thereof. A processing circuit responsive to the biometric signal is adapted to compare the biometric signal with stored biometric data representative of the biometric trait of an enrolled person that is indicative of the identity of the enrolled person. The processor provides a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person. The verification signal is indicative of the enrolled person or the device. A communication unit, including a transmitter circuit, is adapted to transmit the verification signal to a remote host system.

In another aspect, the invention features a personal identification system, comprising: a biometric sensor configured to extract a representation of a biometric trait of a user; a processor configured to verify the user's identity based upon a comparison of a representation of a biometric trait extracted from a user with a stored representation of the biometric trait; and a transmitter configured to transmit a verification signal indicative of a successful verification of the user's identity.

Embodiments may include one or more of the following features. The processor may be configured to process signals received from a global positioning system (GPS) receiver. The processor may be configured to derive trip information (e.g., the location of the GPS receiver) from the signals received from the GPS receiver. The processor may be programmable to prompt the user for additional verification information when the GPS receiver is positioned at a particular location.

The system may include a user input configured to enable a user to enter trip information, and wherein the processor is configured to process information

received from the user. The transmitter may be further configured to transmit signals representative of stored trip information.

The biometric sensor, the processor, and the transmitter may be housed within a portable, hand-held housing. The system may include an input device mounted inside a vehicle and coupled to the vehicle's power system, and wherein the input device is adapted to receive the verification signal from the transmitter and to enable the user to turn on the vehicle only upon receipt of the verification signal. The housing may have the form of a pocket-sized security badge. The housing may be configured to receive a graphical representation of the user.

The system may include an automatic door locking device coupled to a vehicle door (or trunk) and adapted to unlock the door (or trunk) upon receipt of the verification signal. The system also may include a receiver. The processor may be operable to switch the system from a low power operation to a normal power operation when the receiver receives a power-up signal from a host system. The system also may include a memory configured to store the representation of the biometric trait. The memory may be housed within a portable housing separable from the biometric sensor, processor and transmitter.

The communication unit preferably is adapted for remote communication with the host system via a wireless communication medium. The device can further include a display and a keypad.

The biometric sensor system can include a fingerprint sensor, a voice sensor, or any other type of biometric sensor. The fingerprint sensor can include a platen adapted for placing a finger thereon. The fingerprint sensor can further include an optical image sensor, which may include a complementary metal oxide semiconductor (CMOS) optical sensor, a charge coupled device (CCD) optical sensor, or any other optical sensor having sufficient resolution to provide a signal indicative of a fingerprint image. In the embodiments with an optical sensor, the platen would include an optical platen, and the biometric sensor may also include a lens focusing light from the platen onto the optical sensor. The fingerprint sensor can alternatively include a direct contact sensor device, such as a capacitive sensor chip or thermal sensor chip. In these embodiments, the platen would be the surface of the sensor chip.

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.