(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 September 2008 (25.09.2008)

PCT

(10) International Publication Number
WO 2008/113110 A1

(51) International Patent Classification:
G06K 9/00 (2006.01) *H04K 1/00* (2006.01)

(21) International Application Number:
PCT/AU2008/000366

(22) International Filing Date: 14 March 2008 (14.03.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2007901361 16 March 2007 (16.03.2007) AU
2007901683 29 March 2007 (29.03.2007) AU

(71) Applicant *(for all designated States except US)*: **MICROLATCH PTY LTD** [AU/AU]; Unit 13, 145-147 Forest Road, Hurstville, NSW 2220 (AU).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **BURKE, Christopher, John** [AU/AU]; 48 Margate Street, Ramsgate, NSW 2217 (AU).

(74) Agent: **SPRUSON & FERGUSON**; GPO Box 3898, Sydney, NSW 2001 (AU).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(54) Title: METHOD AND APPARATUS FOR PERFORMING A TRANSACTION USING VERIFICATION STATION

(57) Abstract: A method of performing a transaction process using a verification station (127) is disclosed. The method compares a first biometric signature, inputted to a biometric reader (102) incorporated into the verification station (127), to one or more further biometric signatures stored in a memory (124) incorporated into the verification station (127). The method performs the transaction process using card information stored in the memory (124), if the inputted biometric signature matches one of the stored biometric signatures, otherwise, the transaction is not performed. The stored card information was read from a card device (112) and stored in the memory (124) during a previous transaction process using a card device reader (112) incorporated into the verification station (127).

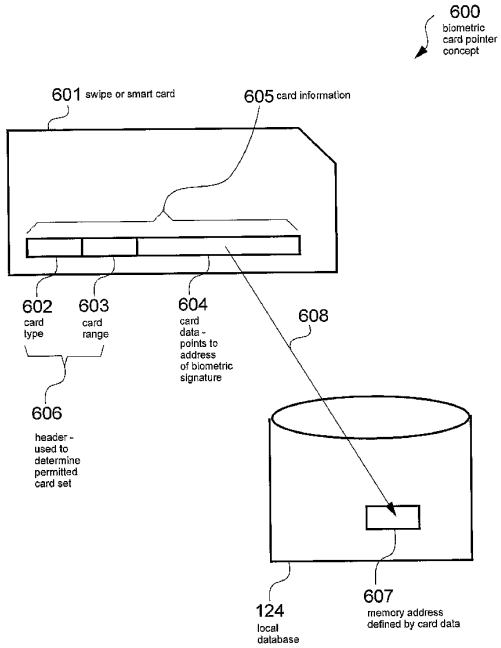

Fig. 4

WO 2008/113110 A1

METHOD AND APPARATUS FOR PERFORMING A TRANSACTION USING A VERIFICATION STATION

Field of the Invention

The present invention relates generally to security issues and, in particular, to security issues associated with use of card devices such as credit cards, smart cards, and wireless card-equivalents such as wireless transmitting fobs.

Background

This description makes reference to various types of "card device" and their associated "reader devices" (respectively referred to merely as cards and readers). The card devices all contain card information that is accessed by "coupling" the card device to an associated reader device. The card information is used for various purposes including drawing cash from an Automatic Teller Machine (ATM), making a purchase on credit, updating a loyalty point account, gaining access to a restricted area or controlled device and so on. The card information is typically accessed from the card by a corresponding card reader which then sends the card information to a "back-end" system that completes the appropriate transaction or process.

One type of card device is the "standard credit card" which in this description refers to a traditional plastic card 701 as depicted in **Fig. 1**. The standard credit card is typically "swiped" through a slot in a standard credit card reader in order to access card information 702 on the card 701. The card information 702 can alternately be encoded using an optical code such as a bar code, in which case the reader is suitably adapted. The standard credit card 701 also typically has the signature 703 of the card-owner written onto a paper strip on the card 701. This is used for verification of the identity of the person submitting the card when conducting a transaction using the card 701.

Another type of card device is the smart card (not shown) that typically has an on-board processor and a memory. The smart card typically has electrical contacts that

mate with corresponding contacts on a smart card reader (not shown) when accessing data in the memory of the smart card.

Still another type of card device is a proximity card (not shown) that typically has an on-board microchip. A proximity card reader sends out a low-level radio frequency (RF) signal, which energizes the microchip embedded in the card when the card is placed in close proximity to the reader. The proximity card then transmits data in the form of a unique code to the reader.

Still another type of card device is the wireless "key-fob" which is a small radio transmitter that emits an RF signal when a button on the fob is pressed. The RF signal can be encoded using the Wiegand protocol, or any other suitable protocol, such as rolling code or Bluetooth™ and can include encryption if desired. The key-fob typically has a processor and memory storing data that is sent via the transmitted signal to a corresponding receiver, which is the "reader device" for this type of card device.

The description also refers to "card user" and "card owner". The card user is the person who submits the card for a particular transaction. The card user can thus be the (authorised) card owner or an (unauthorised) person who has found or stolen the card.

Currently, the above described cards are heavily relied on both for financial transactions, as described above, and also for secure access. However, the cards are often used fraudulently. For example, a card may be used without the consent of the card owner to gain access to a bank account. Further, data stored on a card may be copied and used to gain access to a building or the like.

Clearly the signature 703 on the standard credit card 701 in **Fig. 1** can be forged. Thus, if the standard card 701 is stolen or lost, an unauthorised user can use the card provided that they can supply a sufficiently accurate version of the signature 703. The only recourse available to the card owner is to notify the card issuing company to "cancel" the card.

Current card devices such as the standard credit card, the smart card and the key-fob can have their security enhanced by requiring the card user to provide PIN (Personal Identification Number) information through a keypad to verify their identity prior to completing a transaction. However, PIN information can also be "stolen" by surveillance of the card owner's hands as the card owner operates the keypad.

Biometric verification can also be incorporated into current card systems to enhance security. In **Fig. 2** the card user swipes the standard card 701 through an associated card reader (not shown) that accesses the card information 702 on the card 701. The card user also provides a biometric signature 801, for example by pressing their thumb against a biometric (e.g., fingerprint) reader 802. The card information 702 that is read by the card reader (not shown), together with the biometric signature that is read by the biometric (fingerprint) reader 802, are sent, as depicted by a dashed arrow 803, a computer network 804, and a further dashed arrow 805, to a back-end system including a database 806 and associated processor (not shown).

In this arrangement, the card owner needs to have previously registered their biometric signature 801 and the card information 702 for pre-loading onto the back-end database 806. Having done so, the back-end processor (not shown) compares the pre-loaded information on the database 806 with the information received at 805, in order to check that the card holder of the card 701 is the (authorised) card owner and that the card itself is valid, in which case the transaction in question can proceed. Clearly this arrangement requires a central repository (806) of card information 702 and biometric signatures 801. This is cumbersome and potentially compromises the privacy and security of the holder of the card 701. This arrangement also requires complex back-end database management and the communications network 804. Furthermore, the front-end biometric signature reader 802 requires storage and/or processing capabilities for the biometric signatures. This results in a complex and expensive solution.

Privacy concerns have also been raised against the arrangement of **Fig. 2** which involves centralised storage and processing of personal information including biometric information. These concerns have slowed widespread use of biometrics to enhance user verification.

Another disadvantage of the arrangement of Fig. 2 is that even once the card owner's biometric signature 801 and card information 702 has be pre-loaded onto the back-end database 806, the card owner is still required to carry the card and to validate the card for each transaction. This is inconvenient as the card is often lost or damaged.

Summary

It is an object of the present invention to substantially overcome, or at least ameliorate, one or more disadvantages of existing arrangements.

Disclosed are arrangements which seek to address the above problems by automatically storing a card user's biometric signature in a local memory in a verification station comprising a card reader, a biometric signature reader, the local biometric signature memory (preferably in a mechanically and electronically tamper-proof form), an alphanumeric keypad (optional), and a communication module for communicating with back-end system that may be remotely accessible over a network.

As described herein, when the description refers to "the storing of a biometric signature" in a memory, a person skilled in the art would understand that rather than the actual biometric signature it is a representation of the biometric signature that is actually stored in the memory. This representation may be referred to as a "biometric template" or "template".

The card user's biometric signature is automatically stored the first time the card user uses the verification station in question (this being referred to as the enrolment phase). The biometric signature is stored at a memory address together with a copy of the

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.