ASSA ABLOY AB, et al v CPC Patent Technologies Pty Ltd

IPR2022-01093

IPR2022-01094

HEARING: NOVEMBER 9, 2023

Patent Owner's Slides – Not Evidence

Petitioner's Grounds 1 & 2

Ground	Prior Art	Statutory Basis	Claims
1	Hsu and Sanford	§103	1, 2, 13, 14, 19, and 20
2	Hsu, Sanford, and Tsukamura	§103	1, 2, 13, 14, 19, and 20

Source: Petition at p. 3

Claim 1

1. A method of enrolling in a biometric card pointer system, the method comprising the steps of

receiving card information;

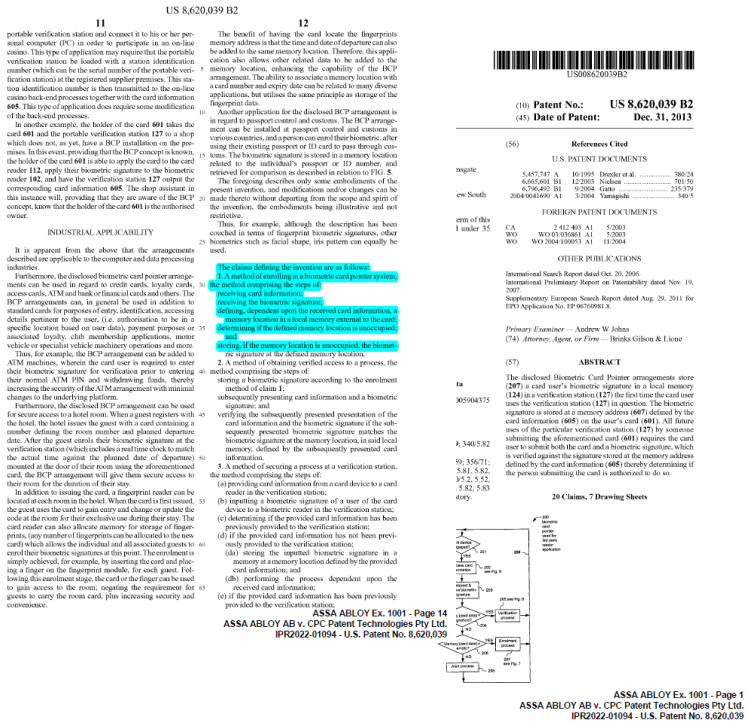
receiving the biometric signature:

defining, dependent upon the received card information, a memory location in a local memory external to the card;

determining if the defined memory location is unoccupied;

and

storing, if the memory location is unoccupied, the biometric signature at the defined memory location.



US 8,620,039 B2

11 12

portable verification station and connect it to his or her personal computer (PC) in order to participate in an on-line casino. This type of application may require that the portable verification station be loaded with a station identification number (which can be the serial number of the portable verification station) at the registered supplier premises. This station identification number is then transmitted to the on-line casino back-end processes together with the card information **605**. This type of application does require some modification of the back-end processes.

In another example, the holder of the card **601** takes the card **601** and the portable verification station **127** to a shop which does not, as yet, have a BCP installation on the premises. In this event, providing that the BCP concept is known, the holder of the card **601** is able to apply the card to the card reader **112**, apply their biometric signature to the biometric reader **102**, and have the verification station **127** output the corresponding card information **605**. The shop assistant in this instance will, providing that they are aware of the BCP concept, know that the holder of the card **601** is the authorised owner.

INDUSTRIAL APPLICABILITY

It is apparent from the above that the arrangements described are applicable to the computer and data processing industries.

Furthermore, the disclosed biometric card pointer arrangements can be used in regard to credit cards, loyalty cards, access cards, ATM and bank or financial cards and others. The BCP arrangements can, in general be used in addition to standard cards for purposes of entry, identification, accessing details pertinent to the user, (i.e. authorisation to be in a specific location based on user data), payment purposes or associated loyalty, club membership applications, motor vehicle or specialist vehicle machinery operations and more.

Thus, for example, the BCP arrangement can be added to ATM machines, wherein the card user is required to enter their biometric signature for verification prior to entering their normal ATM PIN and withdrawing funds, thereby increasing the security of the ATM arrangement with minimal changes to the underlying platform.

Furthermore, the disclosed BCP arrangement can be used for secure access to a hotel room. When a guest registers with the hotel, the hotel issues the guest with a card containing a number defining the room number and planned departure date. After the guest enrols their biometric signature at the verification station (which includes a real time clock to match the actual time against the planned date of departure) mounted at the door of their room using the aforementioned card, the BCP arrangement will give them secure access to their room for the duration of their stay.

In addition to issuing the card, a fingerprint reader can be located at each room in the hotel. When the card is first issued, the guest uses the card to gain entry and change or update the code at the room for their exclusive use during their stay. The card reader can also allocate memory for storage of fingerprints, (any number of fingerprints can be allocated to the new card) which allows the individual and all associated guests to enrol their biometric signatures at this point. The enrolment is simply achieved, for example, by inserting the card and placing a finger on the fingerprint module, for each guest. Following this enrolment stage, the card or the finger can be used to gain access to the room; negating the requirement for guests to carry the room card, plus increasing security and convenience.

The benefit of having the card locate the fingerprints memory address is that the time and date of departure can also be added to the same memory location. Therefore, this application also allows other related data to be added to the memory location, enhancing the capability of the BCP arrangement. The ability to associate a memory location with a card number and expiry date can be related to many diverse applications, but utilises the same principle as storage of the fingerprint data.

Another application for the disclosed BCP arrangement is in regard to passport control and customs. The BCP arrangement can be installed at passport control and customs in various countries, and a person can enrol their biometric, after using their existing passport or ID card to pass through customs. The biometric signature is stored in a memory location related to the individual's passport or ID number, and retrieved for comparison as described in relation to FIG. **5**.

The foregoing describes only some embodiments of the present invention, and modifications and/or changes can be made thereto without departing from the scope and spirit of the invention, the embodiments being illustrative and not restrictive.

Thus, for example, although the description has been couched in terms of fingerprint biometric signatures, other biometrics such as facial shape, iris pattern can equally be used.

The claims defining the invention are as follows:

1. A method of enrolling in a biometric card pointer system, the method comprising the steps of:

receiving card information;

receiving the biometric signature;

defining, dependent upon the received card information, a memory location in a local memory external to the card;

determining if the defined memory location is unoccupied; and

storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

2. A method of obtaining verified access to a process, the method comprising the steps of:

storing a biometric signature according to the enrolment method of claim **1**;

subsequently presenting card information and a biometric signature; and

verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

3. A method of securing a process at a verification station, the method comprising the steps of:

(a) providing card information from a card device to a card reader in the verification station;

(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

(c) determining if the provided card information has been previously provided to the verification station;

(d) if the provided card information has not been previously provided to the verification station;

(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

(db) performing the process dependent upon the received card information;

(e) if the provided card information has been previously provided to the verification station;

ASSA ABLOY Ex. 1001 - Page 14
ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd.
IPR2022-01094 - U.S. Patent No. 8,620,039

US008620039B2

(10) **Patent No.: US 8,620,039 B2**
(45) **Date of Patent: Dec. 31, 2013**

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,457,747 A 10/1995 Drexler et al. 380/24
6,665,601 B1 12/2003 Nielsen 701/50
6,796,492 B1 9/2004 Gitis 235/379
2004/0041690 A1 3/2004 Yamagishi 340/5

FOREIGN PATENT DOCUMENTS

CA 2 412 403 A1 5/2003
WO WO 03/030861 A1 5/2003
WO WO 2004/100053 A1 11/2004

OTHER PUBLICATIONS

International Search Report dated Oct. 20, 2006.
International Preliminary Report on Patentability dated Nov. 19, 2007.
Supplementary European Search Report dated Aug. 29, 2011 for EPO Application No. EP 06760981.8.

Primary Examiner — Andrew W Johns
(74) *Attorney, Agent, or Firm* — Brinks Gilson & Lione

(57) **ABSTRACT**

The disclosed Biometric Card Pointer arrangements store (**207**) a card user's biometric signature in a local memory (**124**) in a verification station (**127**) the first time the card user uses the verification station (**127**) in question. The biometric signature is stored at a memory address (**607**) defined by the card information (**605**) on the user's card (**601**). All future uses of the particular verification station (**127**) by someone submitting the aforementioned card (**601**) requires the card user to submit both the card and a biometric signature, which is verified against the signature stored at the memory address defined by the card information (**605**) thereby determining if the person submitting the card is authorized to do so.

20 Claims, 7 Drawing Sheets

ASSA ABLOY Ex. 1001 - Page 1
ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd.
IPR2022-01094 - U.S. Patent No. 8,620,039

Source: Ex. 1001 ('039 Patent) at Claim 1

Claim 2

2. A method of obtaining verified access to a process, the method comprising the steps of:

storing a biometric signature according to the enrolment **method of claim 1**;

subsequently presenting card information and a biometric signature; and

verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

US 8,620,039 B2

11 12

portable verification station and connect it to his or her personal computer (PC) in order to participate in an on-line casino. This type of application may require that the portable verification station be loaded with a station identification number (which can be the serial number of the portable verification station) at the registered supplier premises. This station identification number is then transmitted to the on-line casino back-end processes together with the card information **605**. This type of application does require some modification of the back-end processes.

In another example, the holder of the card **601** takes the card **601** and the portable verification station **127** to a shop which does not, as yet, have a BCP installation on the premises. In this event, providing that the BCP concept is known, the holder of the card **601** is able to apply the card to the card reader **112**, apply their biometric signature to the biometric reader **102**, and have the verification station **127** output the corresponding card information **605**. The shop assistant in this instance will, providing that they are aware of the BCP concept, know that the holder of the card **601** is the authorised owner.

INDUSTRIAL APPLICABILITY

It is apparent from the above that the arrangements described are applicable to the computer and data processing industries.

Furthermore, the disclosed biometric card pointer arrangements can be used in regard to credit cards, loyalty cards, access cards, ATM and bank or financial cards and others. The BCP arrangements can, in general be used in addition to standard cards for purposes of entry, identification, accessing details pertinent to the user, (i.e. authorisation to be in a specific location based on user data), payment purposes or associated loyalty, club membership applications, motor vehicle or specialist vehicle machinery operations and more.

Thus, for example, the BCP arrangement can be added to ATM machines, wherein the card user is required to enter their biometric signature for verification prior to entering their normal ATM PIN and withdrawing funds, thereby increasing the security of the ATM arrangement with minimal changes to the underlying platform.

Furthermore, the disclosed BCP arrangement can be used for secure access to a hotel room. When a guest registers with the hotel, the hotel issues the guest with a card containing a number defining the room number and planned departure date. After the guest enrols their biometric signature at the verification station (which includes a real time clock to match the actual time against the planned date of departure) mounted at the door of their room using the aforementioned card, the BCP arrangement will give them secure access to their room for the duration of their stay.

In addition to issuing the card, a fingerprint reader can be located at each room in the hotel. When the card is first issued, the guest uses the card to gain entry and change or update the code at the room for their exclusive use during their stay. The card reader can also allocate memory for storage of fingerprints, (any number of fingerprints can be allocated to the new card) which allows the individual and all associated guests to enrol their biometric signatures at this point. The enrolment is simply achieved, for example, by inserting the card and placing a finger on the fingerprint module, for each guest. Following this enrolment stage, the card or the finger can be used to gain access to the room; negating the requirement for guests to carry the room card, plus increasing security and convenience.

The benefit of having the card locate the fingerprints memory address is that the time and date of departure can also be added to the same memory location. Therefore, this application also allows other related data to be added to the memory location, enhancing the capability of the BCP arrangement. The ability to associate a memory location with a card number and expiry date can be related to many diverse applications, but utilises the same principle as storage of the fingerprint data.

Another application for the disclosed BCP arrangement is in regard to passport control and customs. The BCP arrangement can be installed at passport control and customs in various countries, and a person can enrol their biometric, after using their existing passport or ID card to pass through customs. The biometric signature is stored in a memory location related to the individual's passport or ID number, and retrieved for comparison as described in relation to FIG. **5**.

The foregoing describes only some embodiments of the present invention, and modifications and/or changes can be made thereto without departing from the scope and spirit of the invention, the embodiments being illustrative and not restrictive.

Thus, for example, although the description has been couched in terms of fingerprint biometric signatures, other biometrics such as facial shape, iris pattern can equally be used.

The claims defining the invention are as follows:

1. A method of enrolling in a biometric card pointer system, the method comprising the steps of:
receiving card information;
receiving the biometric signature;
defining, dependent upon the received card information, a memory location in a local memory external to the card;
determining if the defined memory location is unoccupied; and
storing, if the memory location is unoccupied, the biometric signature at the defined memory location.

2. A method of obtaining verified access to a process, the method comprising the steps of:
storing a biometric signature according to the enrolment method of claim 1;
subsequently presenting card information and a biometric signature; and
verifying the subsequently presented presentation of the card information and the biometric signature if the subsequently presented biometric signature matches the biometric signature at the memory location, in said local memory, defined by the subsequently presented card information.

3. A method of securing a process at a verification station, the method comprising the steps of:
(a) providing card information from a card device to a card reader in the verification station;
(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;
(c) determining if the provided card information has been previously provided to the verification station;
(d) if the provided card information has not been previously provided to the verification station;
(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and
(db) performing the process dependent upon the received card information;
(e) if the provided card information has been previously provided to the verification station;

ASSA ABLOY Ex. 1001 - Page 14
ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd.
IPR2022-01094 - U.S. Patent No. 8,620,039

US008620039B2

ent No.: US 8,620,039 B2
te of Patent: Dec. 31, 2013

References Cited

U.S. PATENT DOCUMENTS

7 A 10/1995 Drexler et al. 380/24
1 B1 12/2003 Nielsen 701/50
2 B1 9/2004 Gatto 235/379
0 A1 3/2004 Yamagishi 340/5

OREIGN PATENT DOCUMENTS

2 412 403 A1 5/2003
3/030861 A1 5/2003
004/100053 A1 11/2004

OTHER PUBLICATIONS

earch Report dated Oct. 20, 2006.
'eliminary Report on Patentability dated Nov. 19,
European Search Report dated Aug. 29, 2011 for
on No. EP 06760981.8.

ainer — Andrew W Johns
t, Agent, or Firm — Brinks Gilson & Lione

ABSTRACT

d Biometric Card Pointer arrangements store user's biometric signature in a local memory ification station (**127**) the first time the card user ication station (**127**) in question. The biometric tored at a memory address (**607**) defined by the tion (**605**) on the user's card (**601**). All future articular verification station (**127**) by someone e aforementioned card (**601**) requires the card t both the card and a biometric signature, which ainst the signature stored at the memory address e card information (**605**) thereby determining if bmitting the card is authorized to do so.

20 Claims, 7 Drawing Sheets

ASSA ABLOY Ex. 1001 - Page 1
ASSA ABLOY AB v. CPC Patent Technologies Pty Ltd.
IPR2022-01094 - U.S. Patent No. 8,620,039

Source: Ex. 1001 ('039 Patent) at Claim 2

Claim 3

3. A method of securing a process at a verification station, the method comprising the steps of:

(a) providing card information from a card device to a card reader in the verification station;
(b) inputting a biometric signature of a user of the card device to a biometric reader in the verification station;

(c) determining if the provided card information has been previously provided to the verification station;

(d) if the provided card information has not been previously provided to the verification station;

(da) storing the inputted biometric signature in a memory at a memory location defined by the provided card information; and

(db) performing the process dependent upon the received card information;

(e) if the provided card information has been previously provided to the verification station;

(ea) comparing the inputted biometric signature to the biometric signature stored in the memory at the memory location defined by the provided card information;

(eb) if the inputted biometric signature matches the stored biometric signature, performing the process dependent upon the received card information; and

(ec) if the inputted biometric signature does not match the stored biometric signature, not performing the process dependent upon the received card information.

Source: Ex. 1001 ('039 Patent) at Claim 3

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.