Title: MULTIPLE FINGER FINGERPRINT AUTHENTICATION DEVICE

Abstract: A fingerprint authentication device (102), comprises a fingerprint sensor (130), a display interface (140) for indicating a digit of a hand to be presented to the fingerprint sensor (130), and a fingerprint authentication module (120) configured to determine whether a fingerprint scanned by the fingerprint sensor (130) matches a fingerprint template stored by the device and corresponding to the indicated digit.
MULTIPLE FINGER FINGERPRINT AUTHENTICATION DEVICE

The present invention relates to a fingerprint authentication device, and particularly to an RFID fingerprint authentication device storing fingerprint templates for multiple fingers of a single user.

Fingerprint access cards can be used to enhance the security of access control systems. In such a system, employees who are authorised to be in a physical facility carry cards that are linked to a database within the system. A card reader is attached close to a door of the building, and to gain access the employee must present a valid card to the reader. When a card is presented, the reader sends the code from the card to a central computer (commonly called the "panel") which contains the codes of the employee population and the access privileges that they have. If the code corresponds to an authorised employee, then access is granted.

When using fingerprint access cards, the owner of a new card must first enrol their fingerprint into a database of templates within the card. After enrolment, when the card is presented to the card reader at the door, the user must present the corresponding finger or thumb to the fingerprint reader on the card. If a valid finger or thumb is not presented, then the code is not transmitted and access will not be granted.

There are various ways to fool the access system into granting unauthorised access within the facility. The first and most obvious is for a card to become disconnected from its owner, either with the consent of the owner or not. The use of cards having an in-built fingerprint sensor significantly reduces this problem. However, a need still exists for improved security.

The present invention provides a portable fingerprint authentication device, comprising: a fingerprint sensor; a display interface for indicating a digit of a hand to be presented to the fingerprint sensor; and a fingerprint authentication module configured to authenticate the identity of a bearer of the device by determining whether a fingerprint scanned by the fingerprint sensor matches a fingerprint template stored by the device and corresponding to the indicated digit.

The present invention therefore provides improved security because, even if an unauthorised person obtains the device and a duplicate of one of the authorised users' fingerprints, the unauthorised person cannot consistently use the device because the fingerprint may not be the one indicated for a particular authentication.
As used herein, the term "portable" should be understood to distinguish from fixed scanners, for example those mounted to a wall or larger device. In various embodiments, the portable fingerprint authentication device may have a mass of less than 100 grams and/or a volume of less than 100 cubic centimetres. The device may be in the form of a card, a fob, or the like.

In various embodiments, the device may contain a memory storing a fingerprint template for all (five) digits of one hand of a user, and preferably all (ten) digits of both hand of a user. The more fingerprints of the user are held, the more difficult it is for an unauthorised user to obtain all of the fingerprints required to consistently use the device.

In one embodiment the device is configured such that, if a match is not determined, the display interface will indicate the same digit until a match is determined and/or a predetermined period of time has elapsed. This prevents an unauthorised user having one fingerprint from simply repeatedly attempting to use the device until the desired fingerprint is indicated. Of course, in an alternative embodiment, the device may be configured such that if a match is not determined, then the device will indicate a different digit.

The device may further be configured such that, if a match is determined, then the device will indicate a different digit for a subsequent authentication attempt. This ensures that a different digit is required for each successive authentication, reducing the risk of an unauthorised person being able to consistently use the device.

In one embodiment, the device is configured such that, responsive to determining a match, the display interface will indicate a second, different digit to be presented to the fingerprint sensor, wherein the authentication of the bearer further requires determining that a second fingerprint scanned by the fingerprint sensor matches a second fingerprint template stored by the device and corresponding to the second indicated digit. In various implementations, a series of three or more different fingerprint matches may be required for authentication. This ensures that a single fingerprint can never be used to activate the device.

The device may further comprise a wireless communication module for wireless communication with a receiving device external to the fingerprint authentication device, wherein the fingerprint authentication device is configured to wirelessly transmit a code or message to the receiving device responsive to authenticating the bearer. Preferably, the wireless communication module is
disabled unless the bearer is authenticated, and in various embodiments the communication module may be physically disabled unless the bearer is authenticated, for example by disconnecting a power supply or the like.

In various embodiments, the wireless communication module is an RFID module, and the fingerprint authentication device may, in some embodiments, be a passive RFID device.

The device may further comprise a fingerprint enrolment module configured to generate a fingerprint template for an indicated finger or thumb based on one or more fingerprint(s) scanned from the finger or thumb presented to the fingerprint sensor. The fingerprint authentication module and the fingerprint enrolment module may be modules of a single fingerprint processing unit.

By enrolling the fingerprints directly onto the device, fingerprints may be matched more consistently because the enrolment and matching scans are both carried out by the same sensor. Furthermore, irregularities caused by, for example, inconsistent presentation of the digit to different device can be reduced because the user is likely to present their digit consistently in the same manner for the same device (as opposed to using one device for enrolment and a different one for scanning).

The display interface may include a physical depiction of the digits (fingers and thumb) of one or two hands, and an indicator for indicating one of the digits to be presented to the fingerprint sensor. The indicator may, for example, include a plurality of light sources, each being adjacent to one digit.

The fingerprint authentication device may be any one of: an access card, a payment card (such as a credit card, a debit card or a pre-pay card), a loyalty card, an identity card, and a cryptographic card. Such devices are examples of smart cards.

Although more complex portable computing devices such as mobile phones, tablet computers, or the like could be configured to operate in the manner described, the fingerprint authentication device is preferably a dedicated fingerprint authentication device. That is to say, the device does not provide any processing function other than processing of fingerprints (e.g. matching, and optionally enrolling, of fingerprints), and the primary output of the device is an indication of whether the bearer has been authorised (such as by RFID or the like). In particular, the device is preferably not capable of running application software or the like.
Viewed from a second aspect, the present invention also provides a method of authenticating the bearer of a portable device, comprising: indicating a digit of a hand of the bearer to be presented, using a display interface on the portable device; scanning a digit of the hand of the bearer presented to a fingerprint sensor on the portable device; and authenticating the identity of the bearer by determining whether a fingerprint scanned by the fingerprint sensor matches a fingerprint template stored by the device and corresponding to the indicated digit.

As discussed above, by authenticating the bearer of the portable device in this manner, the risk of incorrectly authenticating the bearer of the device is reduced because the bearer must possess all registered fingerprints of the true user in order to consistently use the device.

In various embodiments, the device stores a fingerprint template for all (five) digits of one hand of a user, or all (ten) digits of both hand of a user.

In one embodiment, if a match is not determined, then the same digit will be indicated until a match is determined and/or a predetermined period of time has elapsed. In another embodiment, if a match is not determined, then a different digit will be indicated.

In some embodiments, the step of authentication further comprises: responsive to determining a match, indicating a second, different digit to be presented to the fingerprint sensor, scanning a second digit of the bearer presented to a fingerprint sensor, and determining whether a second fingerprint scanned by the fingerprint sensor matches a second fingerprint template stored by the device and corresponding to the second indicated digit, wherein the bearer is only identified if a match is determined for both digits.

The method may further comprise wirelessly transmitting a code or message from the portable device to the receiving device responsive to authenticating the bearer. In various embodiments, the wireless communication is RF communication, and preferably backscatter RF communication. Preferably, the wireless communication module is disabled (e.g. physically) unless the bearer is authenticated.

As discussed above, the device may be in the form of a card, a fob, or the like. In various embodiments, the portable device may be any one of: an access card, a payment card (such as a credit card, a debit card or a pre-pay card), a loyalty card, an identity card, a cryptographic card and the like.
Viewed from a third aspect, the present invention also provides a method of fingerprint enrolment, comprising: providing a portable fingerprint authentication device to a user, the device including a fingerprint sensor and a display interface for indicating a digit of a hand; indicating a first digit to be presented to the fingerprint sensor using the display interface; performing one or more scans of a presented digit of the hand of the user using the fingerprint sensor; and generating a fingerprint template for the indicated digit based on the scan(s).

The method preferably comprises repeating the steps of indicating a digit, performing one or more scans, and generating a fingerprint template for each digit of one or both hands of the user. Preferably the/each generated fingerprint template is stored in a memory of the device.

As above, the fingerprint authentication device in the method of both the second and third aspects is preferably a dedicated fingerprint authentication device. That is to say, a processor of the device does not provide any function other than processing of fingerprints (i.e. matching and enrolment of fingerprints), and the primary output of the device is an indication of whether the bearer has been authorised (such as by RFID or the like).

The methods described above in the second and third aspects are preferably implemented using the portable fingerprint authentication device described in the first aspect. Furthermore, the portable fingerprint authentication device may be configured to implement one or both of the methods of the second and third aspects. It should be understood that any preferred features of the device apply also to these methods, and vice versa.

Certain preferred embodiments of the present invention will now be described in greater detail, by way of example only and with reference to the accompanying Figures, in which:

Figure 1 schematically illustrates the architecture of a circuit for a passive RFID fingerprint device storing fingerprint templates for multiple fingers of a user; and

Figure 2 illustrates an external housing of the RFID device.

In Figure 1, the architectures of a powered RFID reader 104 and a passive RFID device 102 of the type that may be used in access control systems are shown.

In operation, the RFID reader 104 transmits an RF (radio-frequency) signal via an antenna 106. The signal is typically at 13.56 MHz for MIFARE® and
DESFire® systems, manufactured by NXP Semiconductors, but may be 125 kHz for lower frequency PROX® products, manufactured by HID Global Corp. This signal is received by an antenna 108 of the RFID device 102.

The antenna 108 comprises a tuned circuit, in this arrangement including a coil and a capacitor, tuned to receive an RF signal from the RFID reader 104. When exposed to the excitation field generated by the RFID reader 104, a voltage is induced across the antenna 108.

The antenna 108 has first and second output lines 122, 124, one at each end of the antenna 108. The output lines of the antenna 108 are connected to the fingerprint authentication engine 120 to provide power to the fingerprint authentication device 120. In this arrangement, a rectifier 126 is provided to rectify the AC voltage received by the antenna 108. The rectified DC voltage is smoothed using a smoothing capacitor and supplied to the fingerprint authentication device 120.

The fingerprint authentication engine 120 includes a processing unit 128 and a fingerprint reader 130, which is preferably an area fingerprint reader 130 as shown in Figure 2. The fingerprint authentication engine 120 in this embodiment is passive, and so is powered only by the voltage output from the antenna 108. The processing unit 128 comprises a microprocessor that is chosen to be of very low power and very high speed, so as to be able to perform biometric matching in a reasonable time. The fingerprint authentication engine 120 also includes a memory (not shown) storing fingerprint data, such as a fingerprint template, for each digit of an authorised bearer of the device 102.

When powered, the fingerprint authentication engine 120 causes a display interface 140 to indicate a specific finger or thumb of the user to be presented for authentication. The indicated digit in this embodiment is randomly selected, but the engine 120 is configured to ensure that the same digit is not used for consecutive authorisations.

The fingerprint authentication engine 120 is arranged to then scan a finger or thumb presented to the fingerprint reader 130 and to compare, using the processing unit 128, the scanned fingerprint to the stored fingerprint data corresponding to the indicated digit. A determination is then made as to whether the bearer of the device 102 is the authorised bearer whose fingerprint data is stored on the memory. The scanning and authentication process is preferably completed as quickly as possible, for example time required for capturing a
fingerprint image and accurately recognising an enrolled finger is ideally less than
one second.

In a simple implementation, the authentication simply comprises determining
whether a single, scanned fingerprint matches the pre-stored fingerprint data for the
indicated digit.

In a more complex implementation, a series of indicated matching digits
may need to be presented. Thus, after the first digit is scanned, the display
interface 140 will indicate a second, different digit to be presented to the fingerprint
sensor 130. Each scanned fingerprint is then compared to the template of the
corresponding indicated digit, and the user is only authorised if all of the fingerprints
match the pre-stored fingerprint data for the respective indicated digit. Three more
different fingerprint matches may be required for authentication in some
implementations.

If the user is authenticated, then the RFID chip 110 is authorised to transmit
a signal to the RFID reader 104. This is achieved in this arrangement by closing a
switch 132 to connect an RFID chip 110 to the antenna 108. The signal received
by an antenna 108 of the RFID device 102 is then passed to an RFID chip 110.

The RFID chip 110 includes a transistor 116, such as the field effect
transistor shown, connected in parallel with the antenna 108, and control logic 114
for controlling the messaging from the chip 110. When the RFID chip 110 is
activated, the received signal is supplied to the control logic 114 for processing (for
example, the received signal may include a request for specific data). Furthermore,
a portion of the received signal is rectified by a bridge rectifier 112, and the DC
output of the rectifier 112 is used to power the (passive) control logic 114.

Data output from the control logic 114 is supplied to the transistor 116. By
switching on and off the transistor 116, a signal is transmitted by the RFID device
102 that can be decoded by suitable control circuits 118 in the reader 104. This
type of signalling is known as backscatter modulation and is characterised by the
fact that the reader 104 is used to power the return message to itself.

If the user is not authenticated, then the device 102 will indicate this to the
user, for example using an indicator 136, 138 such as a red LED or the like. The
user may then attempt authorisation again, or the device 102 may impose a "cool
off" period of time before further authorisation attempts may be made.

The device 102 may be configured to indicate the same digit until either a
match is determined or a predetermined period of time has elapsed since the last
unsuccessful authorisation attempt. This prevents an unauthorised user having one fingerprint from simply repeatedly attempting to use the device until the desired fingerprint is indicated.

Figure 2 shows an exemplary housing 134 of the RFID device 102. The circuit shown in Figure 1 is housed within the housing 134 such that a scanning area of the fingerprint reader 130 and the display interface 140 are exposed from the housing 134.

Prior to use the user of the RFID device 102 must first enrol their fingerprint data onto a "virgin" device 102, i.e. one not including any pre-stored biometric data. This may be done by presenting each finger to the fingerprint reader 130 one or more times, preferably at least three times and usually five to seven times. An exemplary method of enrolment of a fingerprint using a low-power swipe-type sensor is disclosed in WO 2014/068090 A1, which those skilled in the art will be able to adapt to the area fingerprint sensor 130 described herein.

The housing may include indicators for communication with the user of the RFID device, such as LEDs 136, 138 and the display interface 140. During enrolment, the user may be guided by the indicators, which tell the user which finger to enrol and if the fingerprint has been enrolled correctly. The LEDs 136, 138 on the RFID device 102 may communicate with the user by transmitting a sequence of flashes or different coloured flashes consistent with instructions that the user has received with the RFID device 102. The display interface 140 may comprise ten LEDs or similar, each positioned over the image of one digit on a hand, such as shown in the Figures. However, other display interfaces capable of indicating which digit to present could also be used.

After several presentations of a finger, its fingerprint will have been enrolled and the user will be prompted to enter their next fingerprint by the indicators. In various embodiments, the device 102 may be single use, i.e. forever responsive only to its original user. In other embodiments, however, it may be possible to reset the device 102 to enable a new user to enrol their data.

With fingerprint biometrics, one common problem has been that it is difficult to obtain repeatable results when the initial enrolment takes place in one place, such as a dedicated enrolment terminal, and the subsequent enrolment for matching takes place in another, such as the terminal where the matching is required. The mechanical features of the housing around each fingerprint sensor must be carefully designed to guide the finger in a consistent manner each time it is
read. If a fingerprint is scanned with a number of different terminals, each one being slightly different, then errors can occur in the reading of the fingerprint. Conversely, if the same fingerprint sensor 130 is used every time then the likelihood of such errors occurring is reduced.

As described above, the present device 102 includes a fingerprint authentication engine 120 having an on-board fingerprint sensor 130 as well as the capability of enrolling the user, and thus both the matching and enrolment scans may be performed using the same fingerprint sensor 130. As a result, scanning errors can be balanced out because, if a user tends to present their finger with a lateral bias during enrolment, then they are likely to do so also during matching. Thus, the use of the same fingerprint sensor 130 for all scans used with the RFID device 102 significantly reduces errors in the enrolment and matching, and hence produces more reproducible results.

As used herein, the term "passive RFID device" should be understood to mean an RFID device 102 in which the return transmission of the RFID device 102 is powered only by energy harvested from an RF excitation field, for example generated by the RFID reader 104. That is to say, a passive RFID device 102 relies on the RFID reader 104 to supply its power for broadcasting. A passive RFID device 102 would not normally include a battery, although a battery may be included to power auxiliary components of the circuit (but not to broadcast) - such devices are often referred to as "semi-passive RFID devices".

In the present arrangement, the power for the RFID chip 110 and the fingerprint authentication engine 120 is harvested from the excitation field generated by the RFID reader 104, and the RFID device 102 is therefore a passive RFID device. However, in alternative embodiments, the RFID device 102 may be a semi-passive RFID device, for example including a battery for powering the fingerprint authentication engine 120 and/or indicators 136, 138, 140. In further alternative embodiments, the RFID device 102 may be an active/powered RFID device, including a battery used for communication.

Whilst the above embodiments relate to RFID access cards, the RFID device 102 described may also be employed for other applications. For example, it could be alternatively employed as a payments card, such as a credit card, a debit card or a pre-pay card, a loyalty card, an identity card, a cryptographic card, or the like.
CLAIMS:

1. A portable fingerprint authentication device, comprising:
   a fingerprint sensor;
   a display interface for indicating a digit of a hand to be presented to the
   fingerprint sensor; and
   a fingerprint authentication module configured to authenticate the identity of
   a bearer of the device by determining whether a fingerprint scanned by the
   fingerprint sensor matches a fingerprint template stored by the device and
   corresponding to the indicated digit.

2. A portable fingerprint authentication device according to claim 1, wherein
   the device is in the form of a card or a fob.

3. A portable fingerprint authentication device according to claim 1 or 2,
   wherein the device has a mass of less than 100 grams and/or a volume of less than
   100 cubic centimetres.

4. A portable fingerprint authentication device according to claim 1, 2 or 3,
   wherein the device is a passive device configured to harvest power from an RF
   excitation field.

5. A portable fingerprint authentication device according to any preceding
   claim, wherein the display interface comprises a static depiction of the digits of one
   or both hands, and a controllable indicator for indicating one of the depicted digits to
   be presented to the fingerprint sensor.

6. A portable fingerprint authentication device according to any preceding
   claim, wherein the device is configured such that, if a match is not determined, the
   display interface will indicate the same digit for subsequent authentication attempts
   until a reset criterion is fulfilled, such as when a match is determined and/or when a
   predetermined period of time has elapsed.

7. A portable fingerprint authentication device according to any preceding
   claim, wherein the device is configured such that, if a match is determined, then the
device will indicate at least one different digit for a subsequent authentication attempt.

8. A fingerprint authentication device according to any preceding claim, further comprising:

   a wireless communication module for wireless communication with a receiving device external to the fingerprint authentication device,
   wherein the fingerprint authentication device is configured to wirelessly transmit a code or message to the receiving device responsive to authenticating the bearer.

9. A fingerprint authentication device according to claim 8, wherein the wireless communication module is disabled unless the bearer is authenticated.

10. A fingerprint authentication device according to any preceding claim,
    wherein, the device is further configured to indicate a second, different digit to be presented to the fingerprint sensor after the first fingerprint has been scanned, and wherein the authentication of the bearer further requires determining that a second fingerprint scanned by the fingerprint sensor matches a second fingerprint template stored by the device and corresponding to the second indicated digit.

11. A fingerprint authentication device according to any preceding claim, further comprising a fingerprint enrolment module configured to generate a fingerprint template for the indicated digit based on one or more fingerprint(s) scanned from the digit presented to the fingerprint sensor.

12. A fingerprint authentication device according to any preceding claim, wherein the device contains a memory storing a fingerprint template for all digits of one or both hands of a user.

13. A fingerprint authentication device according to any preceding claim, wherein the device is one of: an access card, a payment card, a credit card, a debit card, a pre-pay card, a loyalty card, an identity card, and a cryptographic card.

14. A method of authenticating the bearer of a portable device, comprising:
indicating a digit of a hand of the bearer to be presented using a display
interface on the portable device;
scanning a digit of the hand of the bearer presented to a fingerprint sensor
on the portable device; and
authenticating the identity of the bearer by determining whether a fingerprint
scanned by the fingerprint sensor matches a fingerprint template stored by the
device and corresponding to the indicated digit.

15. A method according to claim 14, wherein the authentication further
comprises:
indicting a second, different digit to be presented to the fingerprint sensor,
scanning a second digit of the bearer presented to a fingerprint sensor, and
determining whether a second fingerprint scanned by the fingerprint sensor
matches a second fingerprint template stored by the device and corresponding to
the second indicated digit, wherein the bearer is only authenticated if a match is
determined for both digits.

16. A method according to claim 14 or 15, further comprising:
wirelessly transmit a code or message from the portable device to the
receiving device responsive to authenticating the bearer.

17. A method according to claim 16, wherein the wireless communication
module is disabled unless the bearer is authenticated.

18. A method of fingerprint enrolment, comprising:
providing a portable fingerprint authentication device to a user, the device
including a fingerprint sensor and a display interface for indicating a digit of a hand;
indicating a first digit to be presented to the fingerprint sensor using the
display interface;
performing one or more scans of a presented digit of the hand of the user
using the fingerprint sensor; and
generating a fingerprint template for the indicated digit based on the scan(s).
19. A method according to claim 18, further comprising repeating the steps of indicating a digit, performing one or more scans, and generating a fingerprint template for each digit of one or both hands of the user.
### INTERNATIONAL SEARCH REPORT

**PCT/EP2016/074415**

**A. CLASSIFICATION OF SUBJECT MATTER**

**INV.** G07C9/00

ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

### C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 2015/227937 AI (GLIES W LLIAM [CA]) 13 August 2015 (2015-08-13)</td>
<td>1-3, 5-19</td>
</tr>
<tr>
<td>Y</td>
<td>abstract paragraph [0008] - paragraph [0099] figures 1-7</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>abstract paragraph [0050] - paragraph [0057]</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>EP 2 192 511 AI (RESEARCH IN MOTION LTD [CA]) 2 June 2010 (2010-06-02)</td>
<td>1-19</td>
</tr>
<tr>
<td></td>
<td>abstract paragraph [0002] - paragraph [0091] figures 1-8</td>
<td></td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:
  - **X**: Document of particular relevance; the claimed invention cannot be considered without the document.
  - **Y**: Document of particular relevance; the claimed invention cannot be considered without the document.
  - **T**: Later document published after the international filing date or priority date and in conflict with the application.

Date of the actual completion of the international search

14 December 2016

Date of mailing of the international search report

23/12/2016

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016

Authorized officer

Pafieda Fernandez, J
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>US 2015227937 A1</td>
<td>13-08-2015</td>
<td>NONE</td>
</tr>
<tr>
<td>US 2005001711 A1</td>
<td>06-01-2005</td>
<td>NONE</td>
</tr>
<tr>
<td>EP 2192511 A1</td>
<td>02-06-2010</td>
<td>CA 2686696 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2192511 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 2626805 A2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2010134248 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2013009748 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 6229906 B1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 9804993 A1</td>
</tr>
<tr>
<td>EP 1953676 A1</td>
<td>06-08-2008</td>
<td>AT 520094 T</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1728192 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP 1953676 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2005207624 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 2005096214 A1</td>
</tr>
</tbody>
</table>