(12) UK Patent Application (19) GB (11) 2531378 (13) A

(43) Date of A Publication 20.04.2016

(21) Application No: 1508281.1

(22) Date of Filing: 14.05.2015

(30) Priority Data:
(31) 62062243 (32) 10.10.2014 (33) US

(71) Applicant(s):
Zwipe AS
(Incorporated in Norway)
Tollbugata 13, Mailbox 361, 0152 Oslo, Norway

(72) Inventor(s):
Jean-Hugues Wendling

(74) Agent and/or Address for Service:
Dehns
St. Bride's House, 10 Salisbury Square, LONDON, EC4Y 8JD, United Kingdom

(51) INT CL:
G06K 19/07 (2006.01) ***G06K 9/00*** (2006.01)

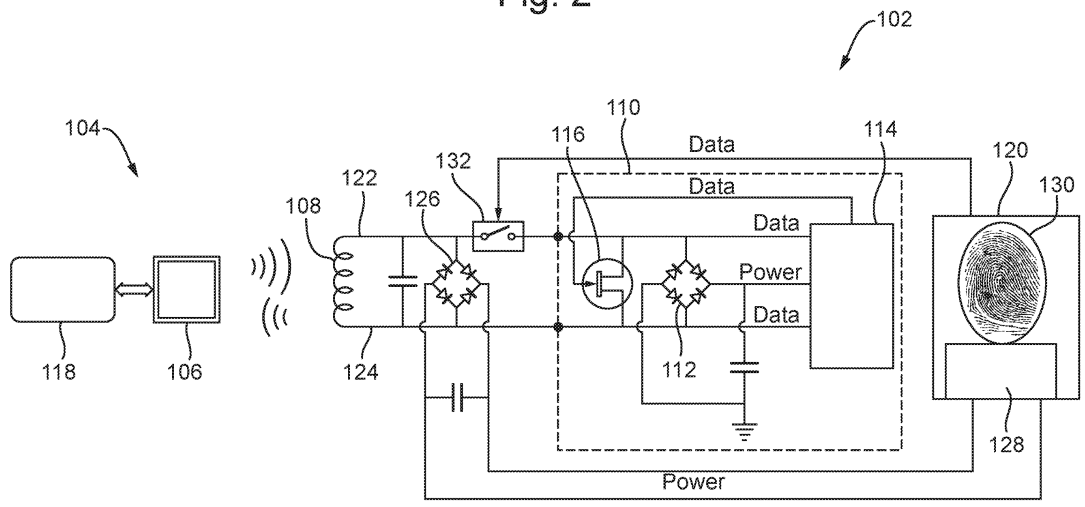
(56) Documents Cited:
US 20150091706 A1
"Zwipe Offers Fingerprint-Authenticated RFID Access-Control Card", Swedberg, RFID Journal 2013, available at: http://www.rfidjournal.com/articles/view?11288/2

(58) Field of Search:
INT CL **G06F, G06K, H02J**
Other: **WPI, EPODOC, INTERNET, TXTE**

(54) Title of the Invention: **Power harvesting**
Abstract Title: **Power harvesting in an RFID device having a biometric authentication engine**

(57) A method of harvesting power in a passive RFID device 102 including a biometric authentication engine 120, comprises receiving a command from a powered RFID reader 104 and supplying power extracted (harvested) from a continuous (non-pulsed) excitation field of the RFID reader 104 to the biometric authentication engine 102 whilst the RFID reader 104 waits for a response to the command. Responsive to determining that a period that the RFID device 102 has been waiting for a response exceeds a predetermined threshold, and that a process being performed by the biometric authentication engine has not been completed, a request for a wait time extension is sent to the RFID reader to cause it to continue supplying the excitation field. The biometric could be a fingerprint 130, and the device could be able to perform both enrolment and matching functions.

Fig. 2



GB 2531378 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

At least some of the priority details shown above were added after the date of filing of the application.

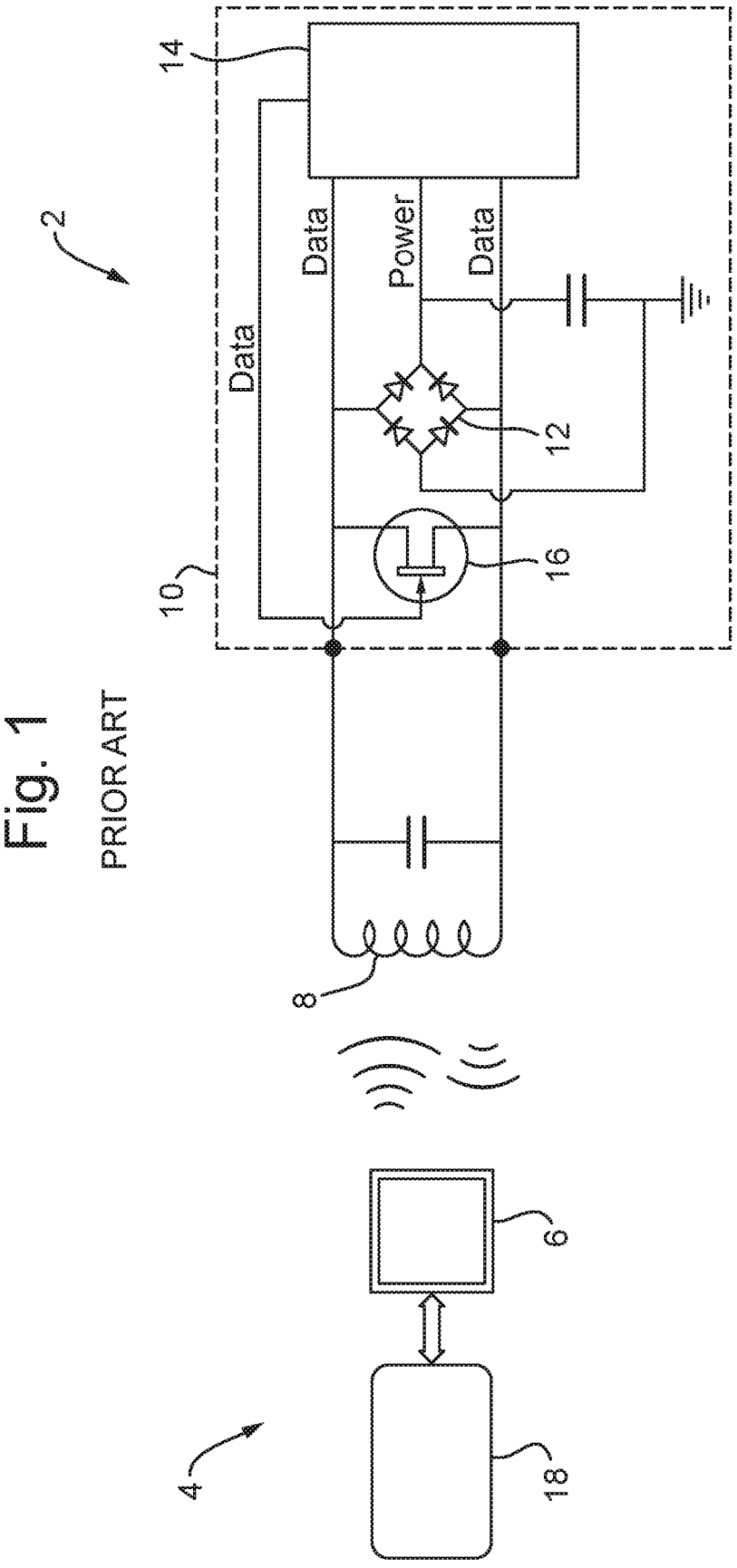
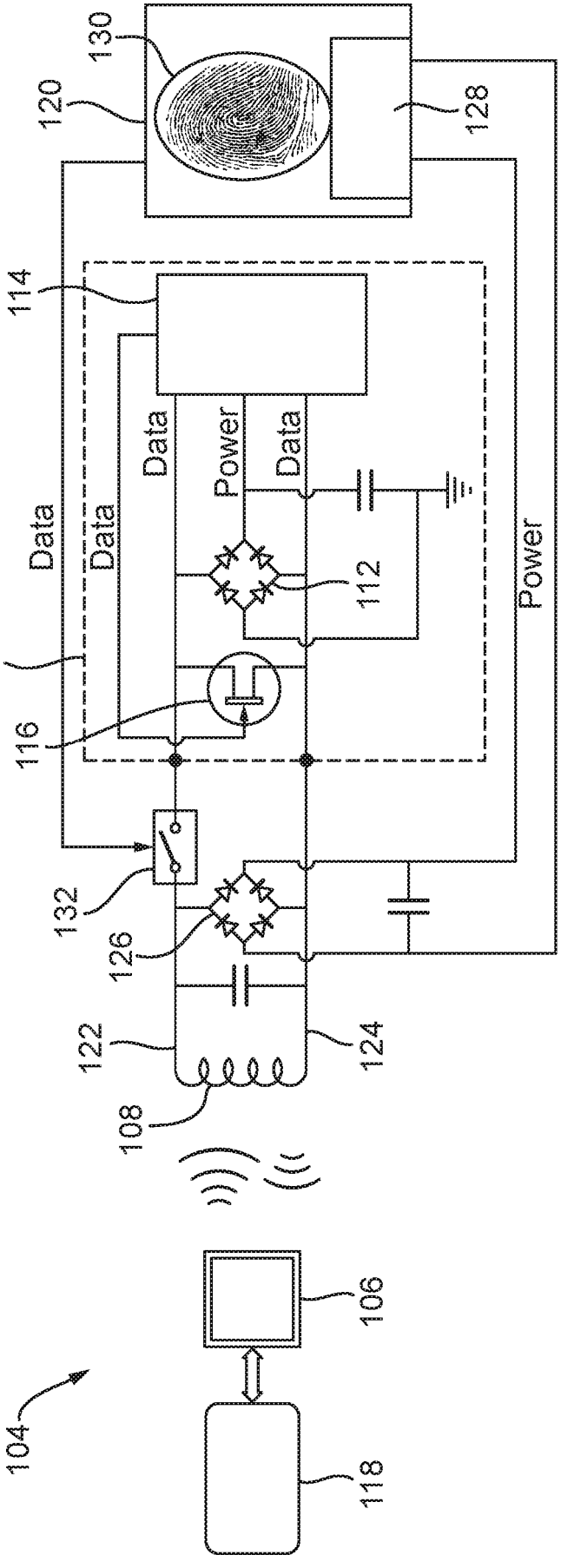


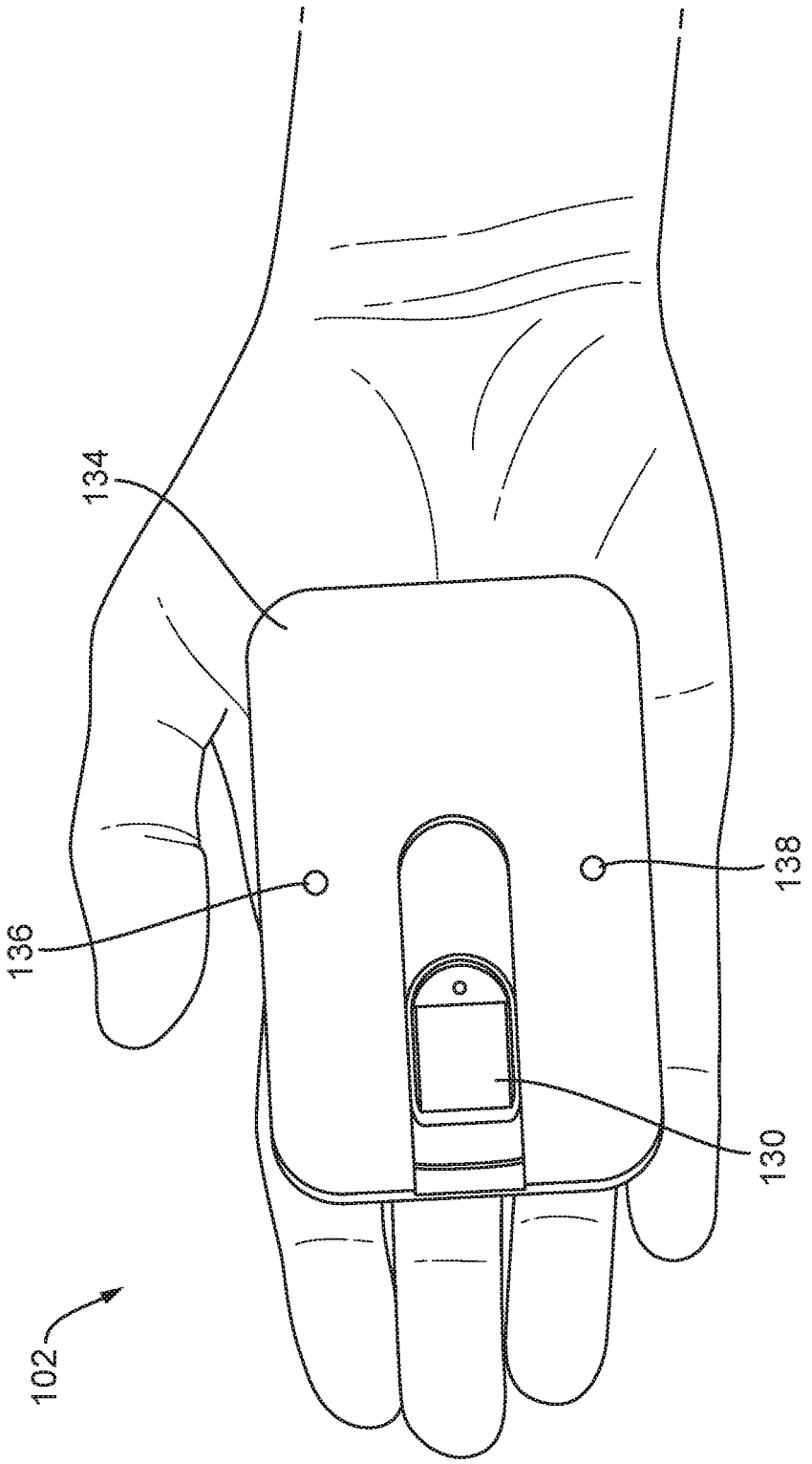
Fig. 1
PRIOR ART

Fig. 2


102
104
106
108
110
112
114
116
118
120
122
124
126
128
130
132
Data
Data
Data
Power
Power

04 11 15

Fig. 3



POWER HARVESTING

The present invention relates to power harvesting in an RFID device, and particularly to power harvesting in a passive RFID device including additional components requiring power such as a fingerprint scanner.

Figure 1 shows the architecture of a typical passive RFID device 2. A powered RFID reader 4 transmits a signal via an antenna 6. The signal is typically 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 8 of the RFID device 2, comprising a tuned coil and capacitor, and then passed to an RFID chip 10. The received signal is rectified by a bridge rectifier 12, and the DC output of the rectifier 12 is provided to control logic 14 that controls the messaging from the chip 10.

Data output from the control logic 14 is connected to a field effect transistor 16 that is connected across the antenna 8. By switching on and off the transistor 16, a signal can be transmitted by the RFID device 2 and decoded by suitable control circuits 18 in the reader 4. This type of signalling is known as backscatter modulation and is characterised by the fact that the reader 4 is used to power the return message to itself.

As an additional security measure, some RFID devices have been adapted to additionally process biometric identification data to provide improved security. In such systems, the user is provided with an RFID card having a biometric template stored on it. A terminal, for example to enable the owner of the card to gain access to money or physical access to a building or office, is provided with a fingerprint sensor and, to authorise the user, a fingerprint read from the terminal is transmitted from the terminal to the RFID card, where a match is performed with the stored template on the card. The RFID card then wirelessly communicates to the terminal the results of the live matching, yes or no.

It is herein proposed to incorporate a biometric sensor, such a fingerprint scanner, into a passive RFID device. At least the preferred embodiments of the present invention seek to solve some of the technical problems associated with such a device.

The present invention provides a method for harvesting power in a passive RFID device comprising a passive biometric authentication engine, the method

comprising: receiving, by the RFID device, a command from a powered RFID reader; receiving, by the RFID device, a non-pulsing continuous radio-frequency excitation field whilst the RFID reader waits for a response to the command; harvesting, by the RFID device, power from the excitation field; supplying the power extracted from the excitation field to the biometric authentication engine; performing a process in the biometric authentication engine, the process being one not required for responding to the command from the RFID reader; determining a period that the RFID device has been waiting for a response; and responsive to determining that the period exceeds a predetermined threshold if the process has not been completed, sending, by the RFID device, a request for a wait time extension to the RFID reader.

As will be discussed in greater detail below, typical RFID readers pulse their excitation signal on and off so as to conserve energy, rather than steadily emitting the excitation signal. Often this pulsing results in a duty cycle of useful energy of less than 10% of the power emitted by steady emission. This may be insufficient to power a biometric authentication engine.

The above method overcomes this problem by taking advantage of certain aspect of the standard functionality of a RFID reader complying with, for example, international standard ISO/IEC 14443. Particularly, whilst the RFID reader waits for a response to a command, it must maintain a non-pulsing, preferably a substantially continuous, radio frequency (RF) excitation field.

Thus, in accordance with this method, when the RFID reader sends a command to the RFID device, the device does not respond, but rather waits and harvests the power to drive the functionality of the biometric authentication engine.

The process performed by the biometric authentication engine is one not required for responding to the command, for example the command may be a "request to provide identification code" command. That is to say, a response to the command from the RFID device is intentionally delayed so as to allow the processing to be performed.

In the preferred embodiments, the RFID device does not respond to the command whilst the biometric authentication engine is performing a process. Furthermore, the method preferably further comprises: after the biometric authentication engine completes the process, responding by the RFID device to the command.

The steps of "determining a period that the RFID device has been waiting for a response; and responsive to determining that the period exceeds a predetermined threshold if the process has not been completed, sending by the RFID device a request for a wait time extension to the RFID reader" are preferably repeated until the process is completed and/or a response to the command has been sent. For example, after the process has been completed, the RFID device may allow the wait time to expire, if no further communication with the RFID reader is required. Alternatively, a response to the RFID reader may be sent, for example if the process was part of an authorisation step before responding to the command.

Preferably, the period is a time since the command was received or since the last wait time extension request was made. Thus, the request for a wait time extension can be sent before expiry of the current wait time to ensure that the RFID reader continues to maintain the RF excitation field until the process is complete.

The process performed by the biometric authentication engine may be one of a biometric enrolment process or a biometric matching process. The described method is particularly applicable to biometric matching or enrolment, for example fingerprint matching or enrolment processes, as these processes require input from the user (i.e. one or more biometric scans), which can only be processed at the rate that they are supplied by the user of the RFID device.

Without using a request for a wait time extension, the maximum default time that a non-pulsing RF excitation field could be supplied is 4.949 seconds for an RFID reader complying with international standard ISO/IEC 14443. Thus, the method allows processes to be performed by the biometric authentication device, wherein the process requires greater than 5.0 seconds to be completed.

In various embodiments, the biometric authentication engine may include a biometric scanner and a processing unit. Preferably, the biometric authentication engine is a fingerprint authentication engine.

As discussed above, the present method is particularly applicable to devices and readers complying with international standard ISO/IEC 14443 (although the method may be applicable also to other standards operating in a similar manner), and thus the RFID device is preferably a proximity integrated circuit card (PICC) and the RFID reader is preferably a proximity coupling device (PCD). The PICC and PCD preferably comply with the definitions set forth in the international standard ISO/IEC 14443.

The predetermined threshold is preferably below a pre-arranged first wait time of the PICC and the PCD.

Viewed from a second aspect, the present invention provides a passive RFID device comprising: an antenna for receiving a radio-frequency excitation field from an RFID reader and for harvesting power from the excitation field; a passive biometric authentication engine arranged to receive power harvested by the antenna; and an RFID device controller arranged to perform a method, comprising: receiving, by the antenna, a command from a powered RFID reader; receiving, by the antenna, a substantially continuous radio-frequency excitation field whilst the RFID reader waits for a response to the command; performing a process in the biometric authentication engine, the process being one not required for responding to the command from the RFID reader; determining a period that the RFID device has been waiting for a response; and responsive to determining that the period exceeds a predetermined threshold if the process has not been completed, sending by the antenna a request for a wait time extension to the RFID reader.

The RFID device controller is preferably further arranged to perform any or all of the preferred steps of the method of the first aspect.

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 illustrates a circuit for a prior art passive RFID device;

Figure 2 illustrates a circuit for a passive RFID device incorporating a fingerprint scanner; and

Figure 3 illustrates an external housing for the passive RFID incorporating the fingerprint scanner.

Figure 2 shows the architecture of an RFID reader 104 and a passive RFID device 102, which is a variation of the prior art passive RFID device 2 shown in Figure 1. The RFID device 102 shown in Figure 2 has been adapted to include a fingerprint authentication engine 120.

The RFID reader 104 is a conventional RFID reader and is configured to generate an RF excitation field using a reader antenna 106. The reader antenna 106 further receives incoming RF signals from the RFID device 102, which are decoded by control circuits 118 within the RFID reader 104.

The RFID device 102 comprises an antenna 108 for receiving an RF (radio-frequency) signal, a passive RFID chip 110 powered by the antenna, and a passive fingerprint authentication engine 120 powered by the antenna.

As used herein, the term "passive RFID device" should be understood to mean an RFID device 102 in which the RFID chip 110 is powered only by energy harvested from an RF excitation field, for example generated by the RFID reader 118. That is to say, a passive RFID device 102 relies on the RFID reader 118 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".

Similarly, the term "passive fingerprint/biometric authentication engine" should be understood to mean a fingerprint/biometric authentication engine that is powered only by energy harvested from an RF excitation field, for example an RF excitation field generated by the RFID reader 118.

The antenna comprises a tuned circuit, in this arrangement including an induction 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 end 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 3. The fingerprint authentication engine 120 is passive, and hence 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 is arranged to scan a finger or thumb presented to the fingerprint reader 130 and to compare the scanned fingerprint of the finger or thumb to pre-stored fingerprint data using the processing

unit 128. A determination is then made as to whether the scanned fingerprint matches the pre-stored fingerprint data. In a preferred embodiment, the time required for capturing a fingerprint image and accurately recognising an enrolled finger is less than one second.

If a match is determined, then the RFID chip 110 is authorised to transmit a signal to the RFID reader 104. In the Figure 2 arrangement, this is achieved by closing a switch 132 to connect the RFID chip 110 to the antenna. The RFID chip 110 is conventional and operates in the same manner as the RFID chip 10 shown in Figure 1 to broadcast a signal via the antenna 108 using backscatter modulation by switch on and off a transistor 116.

Figure 3 shows an exemplary housing 134 of the RFID device 102. The circuit shown in Figure 2 is housed within the housing 134 such that a scanning area of the fingerprint reader 130 is exposed from the housing 134.

Prior to use the user of the RFID device 102 must first enrol his fingerprint date onto a "virgin" device, i.e. not including any pre-stored biometric data. This may be done by presenting his 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 for 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 the LEDs 136, 138 shown in Figure 3. During enrolment, the user may be guided by the indicators 136, 138, which tell the user 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 consistent with instructions that the user he has received with the RFID device 102.

After several presentations, the fingerprint will have been enrolled and the device 102 may be forever responsive only to its original user.

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 is used every time then the likelihood of such errors occurring is reduced.

As described above, the present device 102 includes a fingerprint authentication device 120 having an onboard 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.

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. That is to say, the RFID device 102 is a passive RFID device, and thus has no battery, but instead uses power harvested from the reader 104 in a similar way to a basic RFID device 2.

The rectified output from second bridge rectifier 126 is used to power the fingerprint authentication engine 120. However, the power required for this is relatively high compared to the power demand for the components of a normal RFID device 2. For this reason, is has not previously been possible to incorporate a fingerprint reader 130 into a passive RFID device 102. Special design considerations are used in the present arrangement to power the fingerprint reader 130 using power harvested from the excitation field of the RFID reader 104.

One problem that arises when seeking to power the fingerprint authentication engine 120 is that typical RFID readers 104 pulse their excitation signal on and off so as to conserve energy, rather than steadily emitting the excitation signal. Often this pulsing results in a duty cycle of useful energy of less than 10% of the power emitted by steady emission. This is insufficient to power the fingerprint authentication engine 120.

RFID readers 104 may conform to ISO/IEC 14443, the international standard that defines proximity cards used for identification, and the transmission protocols for communicating with them. When communicating with such RFID devices 104, the RFID device 102 can take advantage of a certain feature of these protocols, which will be described below, to switch the excitation signal from the

RFID reader 104 to continuous for long enough to perform the necessary calculations.

The ISO/IEC 14443-4 standard defines the transmission protocol for proximity cards. ISO/IEC 14443-4 dictates an initial exchange of information between a proximity integrated circuit card (PICC), i.e. the RFID device 102, and a proximity coupling device (PCD), i.e. the RFID reader 104, that is used, in part, to negotiate a frame wait time (FWT). The FWT defines the maximum time for PICC to start its response after the end of a PCD transmission frame. The PICC can be set at the factory to request an FWT ranging from 302 μs to 4.949 seconds.

ISO/IEC14443-4 dictates that, when the PCD sends a command to the PICC, such as a request for the PICC to provide an identification code, the PCD must maintain an RF field and wait for at least one FWT time period for a response from the PICC before it decides a response timeout has occurred. If the PICC needs more time than FWT to process the command received from the PCD, then the PICC can send a request for a wait time extension (S(WTX)) to the PCD, which results in the FWT timer being reset back to its full negotiated value. The PCD is then required to wait another full FWT time period before declaring a timeout condition.

If a further wait time extension (S(WTX)) is sent to the PCD before expiry of the reset FWT, then the FWT timer is again reset back to its full negotiated value and the PCD is required to wait another full FWT time period before declaring a timeout condition.

This method of sending requests for a wait time extension can be used to keep the RF field on for an indefinite period of time. While this state is maintained, communication progress between the PCD and the PICC is halted and the RF field can be used to harvest power to drive other processes that are not typically associated with smart card communication, such as fingerprint enrolment or verification.

Thus, with some carefully designed messaging between the card and the reader enough power can be extracted from the reader to enable authentication cycle. This method harvesting of power overcomes one of the major problem of powering a passive fingerprint authentication engine 120 in a passive RFID device 102, particularly for when a fingerprint is to be enrolled.

Furthermore, this power harvesting method allows a larger fingerprint scanner 130 to be used, and particularly an area fingerprint scanner 130, which outputs data that is computationally less intensive to process.

As discussed above, prior to use of the RFID device 102, the user of the device 102 must first enrol themself on the "virgin" device 102. After enrolment, the RFID device 102 will then be responsive to only this user. Accordingly, it is important that only the intended user is able to enrol their fingerprint on the RFID device 102.

A typical security measure for a person receiving a new credit or chip card via the mail is to send the card through one mailing and a PIN associated with the card by another. However for a biometrically-authenticated RFID device 102, such as that described above, this process is more complicated. An exemplary method of ensuring only the intended recipient of the RFID device 102 is able to enrol their fingerprint is described below.

As above, the RFID device 102 and a unique PIN associated with the RFID device 102 are sent separately to the user. However, the user cannot use the biometric authentication functionality of the RFID card 102 until he has enrolled his fingerprint onto the RFID device 102.

The user is instructed to go to a point of sale terminal which is equipped to be able to read cards contactlessly and to present his RFID device 102 to the terminal. At the same time, he enters his PIN into the terminal through its keypad.

The terminal will send the entered PIN to the RFID device 102. As the user's fingerprint has not yet been enrolled to the RFID device 102, the RFID device 102 will compare the keypad entry to the PIN of the RFID device 102. If the two are the same, then the card becomes enrolable.

The card user may then enrol his fingerprint using the method described above. Alternatively, if the user has a suitable power source available at home, he may take the RFID device 102 home and go through a biometric enrolment procedure at a later time.

The RFID device 102, once enrolled may then be used contactlessly using a fingerprint, with no PIN, or with only the PIN depending on the amount of the transaction taking place.

CLAIMS:

1. A method for harvesting power in a passive RFID device comprising a passive biometric authentication engine, the method comprising:

receiving, by the RFID device, a command from a powered RFID reader;

receiving, by the RFID device, a non-pulsing continuous radio-frequency excitation field whilst the RFID reader waits for a response to the command;

harvesting, by the RFID device, power from the excitation field;

supplying the power extracted from the excitation field to the biometric authentication engine;

performing a process in the biometric authentication engine, the process being one not required for responding to the command from the RFID reader;

determining a period that the RFID device has been waiting for a response; and

responsive to determining that the period exceeds a predetermined threshold, if the process has not been completed, sending, by the RFID device, a request for a wait time extension to the RFID reader.

2. A method according to claim 1, wherein the RFID device does not respond to the command whilst the biometric authentication engine is performing a process.

3. A method according to claim 1 or 2, further comprising:

after the biometric authentication engine completes the process, responding by the RFID device to the command.

4. A method according to any preceding claim, wherein the steps of determining a period and sending a request for a wait time extension to the RFID reader are repeated until the process is completed and/or a response to the command has been sent.

5. A method according to any preceding claim, wherein the period is a time since the command was received or since the last wait time extension request was made.

6. A method according to any preceding claim, wherein the process performed by the biometric authentication engine is a biometric enrolment process.

7. A method according to any of claims 1 to 5, wherein the process performed by the biometric authentication engine is a biometric matching process.

8. A method according to any preceding claim, wherein the process requires greater than 5.0 seconds to be completed.

9. A method according to any preceding claim, wherein the biometric authentication engine includes a biometric scanner and a processing unit.

10. A method according to claim 9, wherein the biometric authentication engine is a fingerprint authentication engine and the biometric scanner is a fingerprint scanner.

11. A method according to any preceding claim, wherein the RFID device is a proximity integrated circuit card (PICC) and the RFID reader is a proximity coupling device (PCD).

12. A method according to claim 11, wherein the predetermined threshold is less than a first wait time (FWT) of the PCD.

13. A passive RFID device comprising:

an antenna for receiving a radio-frequency excitation field from an RFID reader and for harvesting power from the excitation field;

a passive biometric authentication engine arranged to receive power harvested by the antenna; and

an RFID device controller arranged to perform a method, comprising:

receiving, by the antenna, a command from a powered RFID reader;

receiving, by the antenna, a substantially continuous radio-frequency excitation field whilst the RFID reader waits for a response to the command;

performing a process in the biometric authentication engine, the process being one not required for responding to the command from the RFID reader;

determining a period that the RFID device has been waiting for a response; and

responsive to determining that the period exceeds a predetermined threshold if the process has not been completed, sending by the antenna a request for a wait time extension to the RFID reader.

14. A passive RFID device according to claim 13, wherein the RFID controller is configured not to respond to the command whilst the biometric authentication engine is performing a process.

15. A passive RFID device according to claim 13 or 14, wherein the method further comprises:

after the biometric authentication engine completes the process, responding by the RFID device to the command.

16. A passive RFID device according to any of claims 13 to 15, wherein the steps of determining a period and sending a request for a wait time extension to the RFID reader are repeated until the process is completed and/or a response to the command has been sent.

17. A passive RFID device according to any of claims 13 to 16, wherein the period is a time since the command was received or since the last wait time extension request was made.

18. A passive RFID device according to any of claims 13 to 17, wherein the process performed by the biometric authentication engine is a biometric enrolment process.

19. A passive RFID device according to any of claims 13 to 17, wherein the process performed by the biometric authentication engine is a biometric matching process.

20. A passive RFID device according to any of claims 13 to 19, wherein the process requires greater than 5.0 seconds to be completed.

21. A passive RFID device according to any of claims 13 to 20, wherein the biometric authentication engine includes a biometric scanner and a processing unit.

22. A passive RFID device according to claim 21, wherein the biometric authentication engine is a fingerprint authentication engine and the biometric scanner is a fingerprint scanner.

23. A passive RFID device according any preceding claim, wherein the passive RFID device is a proximity integrated circuit card (PICC) and the RFID reader is a proximity coupling device (PCD).

24. A passive RFID device according to any preceding claim, wherein the predetermined threshold is set to be less than a first wait time (FWT) of the PCD.

25. A method substantially as hereinbefore described with reference to Figures 2 and 3 for harvesting power in a passive RFID device.

25. A passive RFID device substantially as hereinbefore described with reference to Figures 2 and 3.

Intellectual Property Office

Application No:	GB1508281.1	**Examiner:**	Alan Phipps
Claims searched:	1-24	**Date of search:**	22 October 2015

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
A	--	"Zwipe Offers Fingerprint-Authenticated RFID Access-Control Card", Swedberg, RFID Journal 2013, available at: http://www.rfidjournal.com/articles/view?11288/2 see whole article
A	--	US 2015/091706 A1 CHEMISHKIAN et al., see whole document, discloses energy harvesting in a RFID device

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{X} :

Worldwide search of patent documents classified in the following areas of the IPC

G06F; G06K; H02J

The following online and other databases have been used in the preparation of this search report

WPI, EPODOC, INTERNET, TXTE

International Classification:

Subclass	Subgroup	Valid From
G06K	0019/07	01/01/2006
G06K	0009/00	01/01/2006
H02J	0017/00	01/01/2006