

SPECIFICATION

TITLE OF INVENTION

SMART CARD FOR PASSPORT, ELECTRONIC PASSPORT, AND METHOD, SYSTEM, AND APPARATUS FOR AUTHENTICATING PERSON HOLDING SMART CARD OR ELECTRONIC PASSPORT

FIELD OF THE INVENTION

[0001] The present invention relates to smart cards and electronic passports. More particularly, the present invention relates to smart cards and electronic passports including a biometric sensor, and method, system, and apparatus for authenticating a person holding the smart card or the electronic passport.

BACKGROUND OF THE INVENTION

[0002] Smart cards, which are also referred to as integrated circuit (IC) cards, typically include a microprocessor and memory on their plastic body, and are capable of data processing required for the specific purpose of the cards. The conventional smart cards are typically "credit-card" sized, and ranging from simple memory-type smart cards storing user identification information to high-end smart cards with a sophisticated computational capacity. Typically, a card reader is used to read the stored information associated with the cardholder, such as a user name, account number, personal identification number (PIN), password, and the like. The card reader may be contact type or contactless type. The authentication process is typically performed after the necessary

information is read from the smart card to the card reader, using the card reader or other authentication device communicating with the card reader, such as a local or remote authentication sever.

[0003] However, such smart cards can be stolen or counterfeited, and the authentication/verification system on which the smart cards are operating can be hacked, and the conventional smart card system is still vulnerable to identity theft and fraud. The ever increasing terrorist threat as well as the explosive rise in the crime of identity theft calls for more robust and protected security systems to authenticate and verify identity of individuals using or holding smart cards. In addition, it is desirable to protect the privacy of the personal information associated with the smart card while providing such a tamper-proof security system.

BRIEF DESCRIPTION OF THE INVENTION

[0004] A smart card authenticates a cardholder. The smart card includes a substrate, a sensor module, a wireless transceiver module, and a power circuit. The sensor module includes (a) a biometric sensor adapted to detect biometric information from a person's body, (b) a processor unit adapted to authenticate the person in response to the detected biometric information and generate an authentication signal representing an authentication result, and (c) a memory adapted to store biometric information of a specific individual associated with the smart card. The wireless transceiver module transmits signals received from the processor unit and receives a wirelessly-transmitted power signal. The power circuit generates at least one supply voltage from the received power signal and provides the supply voltage to the sensor module. An electronic passport is embedded with the smart card, and a terminal module is used for wirelessly transmitting power to and receiving signals from the electronic passport or the smart card.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The accompanying drawings, which are incorporated into and constitute a part of this specification, illustrate one or more embodiments of the present invention and, together with the detailed description, serve to explain the principles and implementations of the invention.

In the drawings:

FIG. 1 is a functional block diagram schematically illustrating a smart card for authenticating a person holding the smart card in accordance with one embodiment of the present invention.

FIG. 2 is a block diagram schematically illustrating an example of the smart card in accordance with one embodiment of the present invention.

FIG. 3 is an electrical block diagram schematically illustrating a power circuit in the smart card in accordance with one embodiment of the present invention.

FIG. 4 is an electrical block diagram schematically illustrating an example of the power circuit in the smart card in accordance with one embodiment of the present invention.

FIG. 5 is an electrical diagram schematically illustrating an example of the implementation of a power portion of the smart card in accordance with one embodiment of the present invention.

FIG. 6 is a process flow diagram schematically illustrating an example of authentication process performed in the processor unit with a fingerprint sensor.

FIG. 7 is an electrical block diagram schematically illustrating an example of the sensor/processor portion of the smart card in accordance with one embodiment of the

present invention.

FIG. 8 is a block diagram schematically illustrating another example of implementation of the processor unit of the smart card having an encryption/decryption scheme.

FIG. 9A is a block diagram schematically illustrating another example of implementation of the processor unit of the smart card in accordance with one embodiment of the present invention.

FIG. 9B is a block diagram schematically illustrating yet another example of implementation of the processor unit of the smart card in accordance with one embodiment of the present invention.

FIG. 10 is a block diagram schematically illustrating a smart card in accordance with one embodiment of the present invention.

FIG. 11 is a diagram schematically illustrating an electronic passport including a smart card in accordance with one embodiment of the present invention.

FIG. 12 is a block diagram schematically illustrating an example of a smart card embedded in the passport shown in FIG. 11.

FIG. 13 is a diagram schematically illustrating an electronic passport in accordance with one embodiment of the present invention, which includes a biometric sensor and a display.

FIG. 14 is a diagram schematically illustrating an example of the electronic passport including a fingerprint sensor and a display and being authenticating a person.

FIGS. 15 and 16 are diagrams schematically illustrating an example of an electronic passport in accordance with one embodiment of the present invention, which

includes an integrated sensor/display.

FIG. 17 is a diagram schematically illustrating a terminal module for authenticating a person holding a smart card or an electronic passport including a smart card, in accordance with one embodiment of the present invention.

FIG. 18 is a diagram schematically illustrating an example of the terminal module in accordance with one embodiment of the present invention.

FIG. 19 is a functional block diagram schematically illustrating a system for authenticating a person holding a smart card or electronic passport in accordance with one embodiment of the present invention.

FIG. 20 is a process flow diagram schematically illustrating a method for authenticating a person holding a smart card, or an electronic passport embedded with the smart card, in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION

[0006] Embodiments of the present invention are described herein in the context of a smart card for passport, an electronic passport, and a method, system, and apparatus for authenticating a person holding a smart card or electronic passport. Those of ordinary skill in the art will realize that the following detailed description of the present invention is illustrative only and is not intended to be in any way limiting. Other embodiments of the present invention will readily suggest themselves to such skilled persons having the benefit of this disclosure. Reference will now be made in detail to implementations of the present invention as illustrated in the accompanying drawings. The same reference indicators will be used throughout the drawings and the following detailed description to refer to the same or like parts.

[0007] In the interest of clarity, not all of the routine features of the implementations described herein are shown and described. It will, of course, be appreciated that in the development of any such actual implementation, numerous implementation-specific decisions must be made in order to achieve the developer's specific goals, such as compliance with application- and business-related constraints, and that these specific goals will vary from one implementation to another and from one developer to another. Moreover, it will be appreciated that such a development effort might be complex and time-consuming, but would nevertheless be a routine undertaking of engineering for those of ordinary skill in the art having the benefit of this disclosure.

[0008] In accordance with one embodiment of the present invention, the components, process steps, and/or data structures may be implemented using various types of operating systems (OS), computing platforms, firmware, computer programs, computer languages, and/or general-purpose machines. The method can be implemented as a programmed process running on processing circuitry. The processing circuitry can take the form of numerous combinations of processors and operating systems, or a stand-alone device. The process can be implemented as instructions executed by such hardware, hardware alone, or any combination thereof. The software may be stored on a program storage device readable by a machine.

[0009] In addition, those of ordinary skill in the art will recognize that devices of a less general purpose nature, such as hardwired devices, field programmable logic devices (FPLDs), including field programmable gate arrays (FPGAs) and complex programmable logic devices (CPLDs), application specific integrated circuits (ASICs), or the like, may also be used without departing from the scope and spirit of the inventive concepts disclosed herein.

[0010] FIG. 1 schematically illustrates a smart card 10 for authenticating a person holding the smart card in accordance with one embodiment of the present invention. As shown in FIG. 1, the smart card 20 includes a substrate 12, a sensor module 14, a power circuit 16, and a wireless transceiver module 18. The sensor module 14, the power circuit 16, and the wireless transceiver module 18 are provided on the substrate 12. The sensor module 14 detects biometric information from the person's body, performs authentication

for the person based on the detected biometric information, and generates an authentication signal indicating the result of the authentication, for example, positive (successfully authenticated) or negative (authentication failed). The power circuit 16 is coupled to the wireless transceiver module 18, and adapted to generate at least one supply voltage from a power signal received by the wireless transceiver module 18. The supply voltage is provided to the sensor module 14.

[0011] The wireless transceiver module 18 is coupled to the sensor module 14 and the power module 16. The wireless transceiver module 18 is adapted to transmit signals received from the sensor module 14, including the authentication signal, and also adapted to receive a wirelessly-transmitted power signal. The wireless transceiver module 18 is capable of transmitting and receiving electromagnetic waves. However, the wireless transceiver module 18 may also be implemented such that it is capable of transmitting and receiving ultrasonic waves, optical waves, infrared waves, and the like.

[0012] FIG. 2 schematically illustrates a smart card 20 in accordance with one embodiment of the present invention. As shown in FIG. 2, a power antenna 22, a signal antenna 24, a power circuit 26, and a sensor module 28 are provided on a substrate 21. The power antenna 22 is coupled to the power circuit 26, and the signal antenna 24 is coupled to the sensor module 28. In this example, the wireless transceiver module (shown in FIG. 1) is formed of the power antenna 22 and the signal antenna 24. The power antenna 22 and the signal antenna 24 can be the same antenna, but in this example, the signal antenna 24 is provided as a separate and independent antenna. The power

antenna **22** receives the wirelessly transmitted power signal, and the power circuit **26** generates at least one supply voltage **27** from the received power signal, which is provided to the sensor module **28**. The signal antenna **24** transmits signals received from the sensor module **28**. In accordance with one embodiment of the present invention, the signal antenna **24** is substantially smaller than the power antenna **22**. Thus, the signals transmitted from the signal antenna **24** have a substantially shorter range of transmission such that the signals are only received in a proximity of the smart card, preventing unauthorized receipt or intercept of the signals.

[0013] As shown in FIG. 2, the sensor module **28** includes a biometric sensor **30**, a processor unit **32**, and a memory **34**. In addition, the sensor module **28** may further include an indicator **36** indicating the authentication result, and a control interface **38** which provides an external access to the processor unit **32**. As shown in FIG. 2, the processor unit **32** is coupled to the biometric sensor **34** and the memory **34**, and to the optional indicator **36** and the control interface **38**. The processor unit **32** is adapted to authenticate a person holding the smart card in response to the biometric information detected by the biometric sensor **30**, and generate an authentication signal representing the result of the authentication. The memory **34** is typically a non-volatile memory, and adapted to store the biometric information of a specific individual associated with the smart card. It should be noted that although the memory **34** is depicted in the drawings external to the processor unit **32**, it may be integrated within the processor unit **32**. The processor unit **32** also includes a volatile memory such as a random access memory

(RAM) to perform authentication, execute instructions and/or process data. In addition, the processor unit **32** may encrypt signals before their wirelessly transmission.

[0014] FIGS. 3 and 4 schematically illustrate examples of the power antenna **22** and the power circuit **26** portion of the smart card in accordance with one embodiment of the present invention. As shown in FIG. 3, the power circuit **26** includes a rectifier **40** coupled to the power antenna **22**, and a regulator **42** coupled to the rectifier **40**. In this example, the regulator **42** generates two supply voltages V1 and V2, for example, 3.3 V and 1.8 V. In accordance with one embodiment of the present invention, as shown in FIG. 4, the wireless transceiver module may include a plurality of power antennas **44** (**44a**, **44b**, ...**44n**), and the power circuit includes a corresponding plurality of regulator circuits **46** (**46a**, **46b**, ..., **46n**) and a regulator **42**. Since each set of the power antenna **44** and the rectifier **46** functions as a current source, these sets can be combined in parallel to form a larger current source to be regulated by the regulator **42**.

[0015] FIG. 5 schematically illustrates an example of the implementation of a power portion **52** including three power antennas **44** (**44a**, **44b**, **44c**), corresponding rectifiers **46** (**46a**, **46b**, **46c**), and a regulator **42**, in accordance with one embodiment of the present invention. As shown in FIG. 5, each of the rectifiers **46** may have a different structure. For example, the rectifier **46** may be a double voltage rectifier, or may include a Schottky diode. Similarly, the regulator **42** may be a dropper regulator, a switching regulator, or a fly back regulator. The regulator **42** may have sub-parts **42a** and **42b**, each corresponding to a different supply voltage. For examples, the first part **42a** provides a

supply voltage of 3.3V, and the second part **42b** provides a supply voltage of 1.8V. The number and levels of the supply voltages are not limited to two, but desired number and levels of the supply voltages may be provided depending on a specific application.

[0016] In addition, in accordance with one embodiment of the present invention, each of the plurality of power antennas **44** may have a turn number less than five (5).

Preferably, each of the power antennas **44** has equal to or less than two (2) turns.

Antennas with a lower turn number have a lower self inductance, allowing a higher current supply and a faster current ramp up (i.e., higher frequency response). Each of the plurality of power antennas **44** may also have approximately the same length. In addition, the power antennas may be arranged such that the inside area of the antenna coil or loop (i.e., the cross section of the magnetic field generated by the power antennas **44**) is maximized. For example, the power antennas are placed along the edges of the smart card. The connection points of the power antennas may be located closely to each other. Each of the power antennas **44** may be formed as an etched or printed pattern on a plastic or paper material. Each of the power antennas **44** may have a width equal to or greater than 2 mm.

[0017] Referring back to FIG. 2, in accordance with one embodiment of the present invention, the biometric sensor **30** may be a fingerprint sensor adapted to detect fingerprint patterns. The fingerprint sensor can be of any type, but it is preferable to use sensors which can reliably detect fingerprint patterns even if being touched by a wet or dirty finger. In addition, it is preferable to use a finger print sensor which can read the

surface profile of a finger, i.e., the shape and distribution of valleys or mountains of the fingerprint patterns. For example, such a fingerprint sensor may include a pressure sensor cell array or scanner, a micro electro mechanical (MEM) array or scanner, a mechanical stress array or scanner, a distance measuring cell array or scanner, a micro switch array or scanner, an elasticity measuring array or scanner, and the like, which mechanically detect the finger skin profile. However, a fingerprint sensor using a capacitance measuring cell array is not preferable, since the capacitance between the finger and the cell array can vary depending on the condition of the finger, such as moisture. In addition, the fingerprint sensor may also measure a temperature profile of finger skins, for example, using an infrared detector array or scanner.

[0018] Furthermore, since the smart card and/or the passport are to be flexible in certain applications, a fingerprint sensor thereon are also preferably flexible. In such an application, the fingerprint sensor may be made using a polymer material as its insulator or substrate, or the both, for example, polyimide, polyethylene terephthalate (PET), Polypropylene (PPT), Polycarbonate, Butadiene, Epoxy, Nylon, Teflon® (polymers of tetrafluoroethylene (PTFE) or polymers of fluorinated ethylene-propylene (FEP)), and the like. However, it is not limited to the polymer material, but a thinned silicon wafer or substrate may also be used, where the wafer may be made of crystalline, polycrystalline, or amorphous silicon. For example, the thickness of the thinned silicon wafer or substrate is preferably less than 200 micron, and more preferably, less than 100 micron. The thinned silicon substrate is adapted to detect and digitize fingerprint patterns, by measuring capacitance, resistance, and the like. The thinning process may include

chemical etching or gas-plasma etching. In addition, the thinned silicon wafer may be backed up with a mechanical stiffener such as hard polymer, glass epoxy, copper clad glass epoxy, BT resin, copper clad BT resin, stainless steel clad or sheet, aluminum clad, or anodized aluminum clad or sheet, or the like. It should be noted that surface profile sensor and flexibility may not always be satisfied at the same time.

[0019] Referring back to FIG. 2, fingerprint templates of a specific individual associated with the smart card are stored in the memory 34. Also, the biometric sensor 30 may be an image sensor such as a charge coupled device (CCD) or metal oxide semiconductor (MOS) adapted to capture an image of the person. For example, such an image to be captured may be a face, an ear, an iris, and/or a retina of the person. However, the image is not limited to these examples, but any image of the person which can be captured as specific patterns uniquely characterizing the person may be used. In addition, the biometric sensor 30 may be a genetic information detector adapted to detect genetic information or characteristics of the person, including DNA, RNA, proteins, enzymes, blood cells, and the like. In any case, the corresponding biometric information templates (predetermined biometric patterns specifying or identifying the person) are stored in the memory 34. In accordance with one embodiment of the present invention, the biometric sensor 30 is located near an edge of the smart card. This arrangement may make it easy to place other desired or necessary items or data on the face of the smart card.

[0020] As described above, the processor unit **32** performs authentication of the person by comparing the detected biometric information with the stored biometric information, and determines if the person holding the smart card is the same person as the specific individual associated with the smart card. The processor unit **32** may also include an encryption circuit (not shown in FIG. 2) adapted to encrypt signals generated in the processor unit **32** before transmitting.

[0021] FIG. 6 schematically illustrates an example of authentication process performed in the processor unit **32** in which fingerprints are used as the biometric information. First, fingerprint patterns of a person to be authenticated (who is holding the smart card) is captured by the fingerprint sensor (**600**). Then, specific characteristics to be used in the comparison are extracted from the captured finger print patterns (**602**). For example, minutiae, space frequency (density), and/or vector of the fingerprint patterns are extracted. These characteristics may be used alone or in combination. The extracted characteristics are compared with the corresponding templates stored in the memory (**604**). If the extracted characteristics are determined to match the templates, the authentication result is positive, i.e., the person is successfully authenticated. If the extracted characteristics are determined to mismatch the templates, the authentication result is negative, i.e., the person fails the authentication. An authentication signal representing the result is generated (**606**), encrypted (**608**), and then transmitted (**610**) via the signal antenna.

[0022] As shown in FIG. 2, the sensor module 28 may further include the indicator 36 coupled to the processor unit 32. The authentication signal may also be supplied to the indicator 36, which indicates the authentication result. In accordance with one embodiment of the present invention, the indicator 36 may include at least one light emitting diode (LED). For example, the indicator 36 has two LEDs with different colors, such as red and green, and if the person is successfully authenticated, the green LED may be illuminated, and if the person fails the authentication, the red LED. In addition, by using the LEDs in combination and/or using a different illumination mode such as blinking intervals, more information can be indicated than the simple pass/fail results corresponding to the number of the LEDs.

[0023] Since a fingerprint sensor captures two-dimensional patterns from a three-dimensional surface of a finger, the detected pattern might be deformed to yield a false result although the person is a rightful owner of the smart card. Thus, by visually indicating the current status or result of the authentication, the rightful owner can adjust his/her finger pressed on the sensor such that the fingerprint patterns are correctly detected. On the other hand, the indication of unsuccessful authentication would dissuade an illegitimate holder of the smart card.

[0024] The indicator 36 is not limited to LEDs. In accordance with one embodiment of the present invention, the indicator 36 may be a liquid crystal display (LCD) adapted to display the authentication result, such as "success", "authenticated", "error", "contact authority", and other suitable messages. The LCD may also display some icons or

symbols. The indicator may also be a sound player adapted to play an audio signal corresponding to the authentication result. For example, the audio signal has a different frequency, different voice message, or different melody depending on the authentication result.

[0025] As shown in FIG. 2, the sensor module 28 may further include the control interface 38 coupled to the processor unit 32, in accordance with one embodiment of the present invention. The control interface 32 is adapted to receive an external control signal so as to configure the processor unit 32. Typically, the control interface 32 is used in the initial configuration of the smart card when it is issued to a specific individual. For example, the external control signal may be used to configure the hardware and/or software of the processor unit 32, upload a program onto the processor unit 32 and/or the memory 34, upload and store the biometric information templates of the specific individual in the memory 34, and the like. An encryption key and other data for the encryption system in the processor unit 32 may also be selected and/or configured using the external control signal during the initial configuration process.

[0026] In addition, additional personal information of the specific individual, such as personal identification information and other personal information related to the user and/or purpose of the smart card may be stored in the memory 34. For example, such personal identification information includes the name, user name, password, personal identification number (PIN), date of birth, place of birth, driver's license number, and the like. A photographic image of the person may also be stored. In addition, other related

information, for example, the issue date of the smart card, the expiration date of the smart card, contact information of the specific individual, and the like, can be stored. If the smart card is used for a passport, for example, the history of travel or port entries, visa status, and the like may also be stored.

[0027] The external connections to the control interface 38 may be disabled after configuring the processor unit 32 and storing the desired information in the memory 34. For example, the external access to the control interface 38 may be physically disconnected. Such physical disconnection may be permanent. Such a disconnection is preferable to prevent unauthorized access and alteration of the configuration and stored data. However, if update of the stored information is necessary or desirable, the external connection to the control interface 38 may be enabled only if the person is successfully authenticated.

[0028] FIG. 7 schematically illustrates an example of the sensor/processor portion in accordance with one embodiment of the present invention. In this example, the processor unit includes an authentication circuit 56 and a dual mode interface circuit 58. The authentication circuit 56 may be implemented in a central processor unit (CPU) with hardware or software, or any combination of hardware and software. That is, the authentication circuit may be realized using a general purpose CPU with specific software, an ASIC, a field programmable logic device (FPLD), or the like. The authentication CPU 56 may include a memory 60 therein and perform the above-described authentication process so as to generate the authentication signal. The

biometric information of the specific individual associated with the smart card, and optional personal information of the specific individual is stored in the memory 60. The memory 60 may be external to the authentication CPU 56. The memory 60 may be a combination of a random access memory (RAM) such as static RAM (SRAM) or dynamic RAM (DRAM), and a programmable read-only memory (PROM), such as an erasable and programmable read-only memory (EPROM), an electrically erasable and programmable read-only memory (EEPROM), a flash memory (or flash PROM), and the like. The RAM is used to cache the data for a software program, program code, program instructions, and the like. The PROM is used to store the authentication program and other application programs, an encryption application and related data and files, such as encryption key, and the above-mentioned biometric information and personal information of a specific individual. Since the software programs and information stored in the PROM should not be altered or tampered, the PROM should be one-time programmable or writable. In the case of an EEPROM or flash memory, its rewritable functionality may be disabled, for example, by fusing wires or fusing drivers.

[0029] Referring back to FIG. 7, the authorization signal is sent to the dual mode interface circuit 58 via a communication bus (wire) 62. The dual mode interface circuit 58 converts the authentication signal received from authentication CPU 56 into a transmission signal suitable for wireless transmission via a signal antenna 64. That is, the dual mode interface circuit 58 is capable of both of the wired and wireless communications. Typically, however, when the wired communication is enabled on one

side, the wireless communication on the other side is disabled, and vice versa. The signal antenna **64** is preferably made substantially smaller than the power antenna.

[0030] In accordance with one embodiment of the present invention, the system may be compatible with the International Organization for Standardization (ISO) standards. For example, the communication bus **62** may be compatible with ISO 7816, and the dual mode interface circuit **58** may be an ISO dual mode interface chip which is compatible with ISO 7816 (for the wired communication) and ISO 14443 (for the wireless communication). However, other ISO standards may be used depending on the application.

[0031] FIG. 7 also schematically illustrates the biometric sensor **66**, the control interface **70**, and an indicator (LEDs in this example) **68**. The control interface **70** may be implemented using an interface complying the Joint Test Action Group (JTAG) standards, which typically provides test access port architecture. As shown in FIG. 7, the smart card may also include an oscillation circuit **72** adapted to generate a clock signal for the system on the substrate. The clock signal (CLK) is supplied directly or indirectly to all elements to operate in accordance with the clock signal, although such clock signal inputs are not depicted in FIG. 7 for simplicity. Alternatively, a clock signal may be generated from the power signal in accordance with one embodiment of the present invention. In this case, the smart card includes a clock antenna adapted to receive the power signal, and a clock circuit coupled to the clock antenna which generates the clock signal from the received power signal. For example, if the wireless transmission of the

power also complies with the ISO 14443, it would have 13.56 MHz oscillation, which may be used to generate the clock signal.

[0032] FIG. 8 schematically illustrates another example of implementation of the processor unit, in which an encryption/decryption scheme is provided. The authentication CPU 56 includes an encryption circuit 72 and encrypts the authentication signal before sending to the dual mode interface circuit 58. Similarly, the dual interface circuit 58 includes a decryption circuit 74 to decrypt the encrypted signal received from the authentication CPU 56. The dual mode interface circuit 58 also includes an encryption circuit 76 adapted to encrypt the transmission signal before wirelessly transmitted via the signal antenna 64.

[0033] FIG. 9A schematically illustrates another example of implementation of the processor unit in accordance with one embodiment of the present invention. In this example, the processor unit includes a simpler read/write CPU 78 and a dual mode CPU 80 which is capable of performing the full authentication process as well as wireless transmission with encryption. As shown in FIG. 9A, the read/write CPU 78 may include an encryption circuit 92. The read/write CPU 78 encrypts and sends the biometric information detected by the biometric sensor 66 to the dual mode CPU 80. The dual mode CPU 80 includes an authentication circuit 84 and a memory 90. The authentication circuit 84 may be implemented by software, hardware, or a combination of software and hardware. The memory 90 is adapted to store the biometric information templates of a specific individual. The dual mode CPU 80 also includes a decryption circuit 86 to

decrypt the encrypted signal (detected biometric information) received from the read/write CPU 78. The dual mode CPU 80 compares the detected biometric information with the templates store in the memory 90, and generates an authentication signal representing the authentication result. The dual mode CPU 80 encrypts the authentication signal using an encryption circuit 88 before wirelessly transmitting the signal via the signal antenna 64.

[0034] FIG. 9B schematically illustrates yet another example of implementation of the processor unit in accordance with one embodiment of the present invention. In this example, the processor unit includes a sensor CPU 79 and a dual mode CPU 81. In this example, the sensor CPU 79 includes a extraction circuit 83 which may be software, hardware, or a combination thereof, and performs characteristics extraction from the biometric information detected by the biometric sensor 66. The extracted characteristics, such as minutiae, space frequency (density), and/or vector of the fingerprint patterns, are preferably encrypted and sent to the dual mode CPU 81. The dual mode CPU 80 includes a mating/authentication circuit 85, an encryption circuit 86, a decryption circuit 88, and a memory 90. The dual mode CPU 81 performs comparison of the extracted characteristics and the stored biometric information templates (matching with the corresponding reference characteristics), and determine if the person succeed or fail the authentication. The matching/authentication circuit 85 may be implemented by software, hardware, or a combination of software and hardware. For example, the matching/authentication circuit 85 may be implemented as an application program written in an object oriented programming language, such as a JAVA™ applet running

on the JCOP smart card operating system, available from International Business Machines Corporation, Armonk, New York.

[0035] As described above, in accordance with one embodiment of the present invention, the additional personal information may be store in the memory **34**, **60**, or **90**. Such additional information can be read and transmitted when the person holding the smart cared is successfully authenticated. For example, the processor unit **32**, the authentication CPU **56**, or the dual mode CPU **80** may further include a retrieval circuit adapted to retrieve the stored additional personal information from the memory if the detected biometric information is determined to match the stored biometric information. In this case, the processor unit **32**, the authentication CPU **56**, or the dual mode CPU **80** further generates a personal information signal representing the personal information of the specific individual. The personal information signal is being encrypted and transmitted via the signal antenna in the similar manner as the authentication signal described above.

[0036] FIG. 10 schematically illustrates a smart card **100** in accordance with one embodiment of the present invention. As shown in FIG. 10, the smart card **100** includes a substrate **102**, a wireless transmission module having a power antenna **104** and a signal antenna **106**, a power circuit **108**, a clock circuit **110**, and a sensor module **112**. The sensor module **112** includes processor unit **114**, a biometric sensor **116**, a memory **118**, an indicator **120**, and a control circuit **122**, similarly to other embodiments described above. These elements may be one of the corresponding elements in the previous

embodiments, and some elements may be optional as described above. In this embodiment, the sensor module 112 further includes a biosensor 124 adapted to detect that the person holding the smart card is alive. For example, if the biometric sensor 116 is a fingerprint sensor, an unauthorized person might use a replica of the person's finger (or the body part cut from the body) to activate the smart card or utilize information stored therein. Thus, it is also important to make sure that a body from which the biometric information is to be detected is part of a live person for additional security.

[0037] In accordance with one embodiment of the present invention, the biosensor 124 may be one of, or any combination of, an oxygen detector, a carbon dioxide detector, a thermometer, a moisture sensor, an infrared sensor, a voice sensor, a brainwave sensor, an electrocardiogram sensor, an electromagnetic field sensor, a Chi sensor, and the like. In addition, the biosensor 124 may also be an elasticity sensor adapted to detect elasticity of a member in contact therewith, or a blood flow sensor adapted to detect a blood flow in a body part in contact therewith. These biosensors may also be used alone or combined with one or more of the above described biosensors. Furthermore, the biosensor 124 may include a bio-response detector adapted to capture a reflex response of the person to a given stimulus. For example, a reflex reaction such as a change in an iris aperture in response to light intensity illuminated thereon can be used, and the biosensor 124 may include an image sensor adapted to capture an image of the iris, and a light emitter adapted to illuminate an eye of the person. If the biometric sensor 116 also includes an image sensor to capture the image of the person for biometric authentication, the biometric sensor 116 and the biosensor 124 may be integrated into one image sensor.

For example, a static image may be processed for the pattern matching, and a motion (reaction) image responding to the stimulus may be processed for the “alive” test.

[0038] The processor unit **114** generates a positive authentication only if the person is successfully authenticated and also determined to be alive. The authentication result and the alive-test result may be indicated using the indicator **120** in a similar manner as described above.

[0039] In accordance with one embodiment of the present invention, the smart card **100** may further include a display **126**, as shown in FIG. 10. The display **126** is coupled to the processor unit **114**, and adapted to display a photographic image including the specific individual's face if the person is authenticated. For example, an application of the smart card is desirable to have a photographic image of the holder of the smart card, such a photographic image can be made available only if a person holding the smart card is successfully authenticated. This feature make counterfeiting the smart card more difficult. The righteous holder's signature may also be displayed with the photographic image. The photographic image and the optional signature to be displayed may be stored in the memory **118**.

[0040] In accordance with one embodiment of the present invention, the biometric sensor **116** and the display **126** may be integrated into one element. For example, the biometric sensor **116** may be substantially transparent and laid on the display **112**. In addition, since the display **126** is activated and display the image only if the holder of the

smart card is successfully authenticated (including passing the live test), the display 112 also functions as an indicator.

[0041] In accordance with one embodiment of the present invention, the smart cards described in the above embodiments are adapted to be embedded in a passport. FIG. 11 schematically illustrates an electronic passport 130 including a smart card in accordance with one embodiment of the present invention. For example, as shown in FIG. 11, the smart card may be embedded in a front or back cover 131 of the passport 130 such that a biometric sensor 132 is visibly arranged on an inner side 134 of the front or back cover 131 where the personal identification information of the passport holder and related data are typically placed. As shown in FIG. 11, an indicator 136 may also be visibly arranged on the inner side 134 of the passport 130, especially if the indicator 136 visually indicates the authentication result, as described above. Preferably, the biometric sensor 132 is placed near an edge of the inner side 134 of the passport 130. Also preferably, the biometric sensor 132 and the optional indicator 136 are placed on the inner side 134 such that the biometric sensor 132 and the optional indicator 136 do not interfere with the passport holder's photograph 138 and other personal data 140 on the inner side 134.

[0042] FIG. 12 schematically illustrates an example of a smart card 150 embedded in the passport 130 shown in FIG. 11. Typically, the size of the smart card 150 is slightly smaller than that of the passport 130. Similarly to the embodiments described above, the smart card 150 includes a wireless transmission module including a power antenna 152 and a signal antenna 154, a power circuit 156, and a sensor module including the

biometric sensor 132, the optional indicator 136, a processor unit having an authentication CPU 158 and a dual mode interface circuit 160, and a control interface 162. The authentication CPU 158 includes a memory (not shown) to store biometric information template and other personal data, as described above. The processor unit may be integrated into one element, or the authentication process may be performed by the dual mode CPU, as described above. In this example, the power antenna 152 includes three independent antennas having a similar length and arranged along the edges of the substrate 164 of the smart card 150.

[0043] Preferably, the signal antenna 154 is substantially smaller than the power antenna 152. For example, the signal antenna 154 (and signal antennas 24 and 64 in the above embodiments) is made small enough to be placed right upon or very close to the loop and/or trace of a terminal module antenna 194 or 199 (see FIGS. 17 and 18) which receives the wireless signals transmitted from the signal antenna 154. That is, when the smart card (or the electronic passport) is placed on the terminal module 190, the signal antenna 154 is in the close vicinity of, or preferably right on, the terminal module antenna 194 or 199 such that small load changes in the signal antenna 154 can be detected by the terminal module antenna. In addition, since the load changes are sufficiently small such that only antennas or any receiver module in the very close vicinity can detect the change, any third party cannot detect the load change for the purpose of tapping. For example, the transmitted signal can be detected at maximum 10 mm distance from the signal antenna location. That is, even on the same passport surface area, or the terminal module surface area, the transmitted signal cannot always be detected.

[0044] The control interface 162 is depicted as an external connection (lead bus) 166 is still enabled. This is typical when the electronic passport 130 is first issued to a specific individual and the smart card 150 embedded therein is under an initial configuration, in which necessary and/or desirable data, information, and/or software such as authentication program, encryption program, are uploaded and stored in a memory through the control interface 166. After such configuration and uploading, the external connection 166 may be cut off to disable access to the control interface 162.

[0045] In accordance with one embodiment of the present invention, the smart card 150 may be used as a card-type electronic passport without being embedded in a conventional paper passport. Since all information related to the passport holder and usage of the passport, which are typically printed or stamped on a conventional passport can be electronically or digitally stored in a memory provided on the smart card, the smart card itself may be implemented as an electronic passport. In this case, an additional surface layer may be provided on the substrate 164 so as to protect antennas and other electronic circuits, and also to provide a space to place visible information on the surface of the smart card. In addition, similarly to the passport 130, the biometric sensor and the optional indicate can be visibly arranged on the surface layer. This card-type electronic passport is also applicable to the following embodiments. That is, the passport or electronic passport described in the embodiments may be either a paper passport embedded with the smart card, or paperless electronic passport implemented as a smart card.

[0046] FIG. 13 schematically illustrates an electronic passport 170 in accordance with one embodiment of the present invention, in which a biometric sensor 172 is provided and also a conventional photographic face image of the passport holder is replaced with a display 174. For example, the smart card 100 (FIG. 10) described above or similar smart card may be embedded in the passport 170. It should be noted the location of the display can be rearranged in the smart card 100 such that the display 126 is placed in a proper or desirable location, for example, in the inner page of the front or back cover of the passport 170. Alternatively, the passport 170 may be a card-type electronic passport without paper pages, as described above.

[0047] FIG. 14 schematically illustrates an example of the electronic passport 170 in which the biometric sensor 172 is a fingerprint sensor. As shown in FIG. 14, when a holder of the passport is successfully authenticated when he or she places his/her finger on the fingerprint sensor 172, the display 174 displays the passport holder's photographic image and optionally his/her signature thereon. Such an imaged and optional signature may be displayed during a predetermined time period after the successful authentication, or while the finger is in contact with the fingerprint sensor 172.

[0048] FIG. 15 schematically illustrates an example of an electronic passport 180 in accordance with one embodiment of the present invention, in which the fingerprint sensor and the display are integrated into a sensor/display 182. When a holder of the passport 180 touches the sensor/display 182, as shown in FIG. 16, detected fingerprint patterns are

used for the authentication process as described above, and if the person is authenticated, the sensor/display displays the passport holder's face image and optionally his/her signature thereon. The sensor/display **182** may display the image and optional signature during a predetermined time period after the successful authentication.

[0049] FIG. 17 schematically illustrates a terminal module **190** for authenticating a person holding a smart card or an electronic passport including a smart card, in accordance with one embodiment of the present invention. The smart card or electronic passport may be any of the smart cards or electronic passports described above. The terminal module includes a support plate **192** and an antenna (terminal module antenna) **194** provided thereon. The support plate **192** is adapted to receive the smartcard or electronic passport and has a size suitable to receive the smart card or the passport. The antenna **194** is adapted to transmit a power to the smart card or electronic passport. The wirelessly transmitted power is received by, for example, the wireless transceiver module **18** of the smart card **10** (FIG. 1) placed on the terminal module **190**. The antenna **194** is also adapted to receive a signal transmitted from the wireless transceiver module of the smart card.

[0050] In accordance with one embodiment of the present invention, the terminal module **190** is designed to used with an electronic passport such as the electronic passport **130** embedded with the smart card **150** as described above. If the electronic passport **130** includes the power antenna **152** and the signal antenna **154**, for example, the antenna **194** is adapted to wirelessly transmit the power signal to be received by the power antenna

152, and also to receive the wireless signal transmitted from the signal antenna 154. Preferably, the terminal module antenna 194 is provided on the support plate 192 such that when the electronic passport (or smart card) is placed on the support plate 192 the signal transmission antenna 154 substantially aligns on the terminal module antenna 194. Typically, the terminal module antenna 194 is substantially larger than the signal antenna 154 of the electronic passport, the signal antenna 145 will be placed on a portion 196 of the antenna 194, as shown in FIG. 17. The signal antenna 145 may be positioned just on the portion 196 or in a very close proximity thereof. Alternatively, as shown in FIG. 18, the terminal module 190 may include a power transmitting antenna 198 and a signal receiving antenna 199 separate from the power transmitting antenna 198. In this case, the signal receiving antenna 199 is placed such that the location matches that of the signal antenna 154 when the electronic passport 130 is placed on the terminal module 190.

[0051] As described above, in accordance with embodiments of the present invention, the biometric information detection and the authentication process using the biometric information are performed on-board (on-card) by the smart card or the electronic passport. That is, the authentication of a cardholder/passport holder is performed without externally communicating the sensitive information such as fingerprint patterns and personal information, and such sensitive information is confined within the smart card or the electronic passport. In the case where the authentication result and related personal information is wirelessly transmitted, the transmission signal has a very short range, typically the order of millimeters, and thus is only received by the terminal module on which the smart card or electronic passport is properly placed. Accordingly, the

authentication process and personal information retrieval can be done locally, and the sensitive information does not have to fly over the air or travel through the network system such as the Internet. In addition, since the full authentication can be performed locally (on-board), it is not affected by any accident or unavailability of access to an external network system or a central database.

[0052] However, under certain circumstances, it may be preferable to communicate the biometric information and/or personal information of an individual with an external system beyond the terminal module. For example, in the airport, the authentication result may be monitored by the airport security personnel, and the authentication result and necessary personal information may be transmitted to a monitoring device/terminal within a local computer network. In addition, in some suspicious cases, the biometric information such as fingerprints may need to be screened against that contained in a criminal record, terrorist list database, immigration records, and the like, which are typically maintained in a government central database. For example, when the smart card or electronic passport might have been counterfeited, all of the information stored in the suspicious smart card or passport may need to be examined and compared against the corresponding information of a legitimate individual as claimed to be. Thus, the terminal module may also have a capability of communicating with outside computer system in accordance with one embodiment of the present invention

[0053] FIG. 19 schematically illustrates a system 300 for authenticating a person holding a smart card or electronic passport in accordance with one embodiment of the

present invention. As shown in FIG. 19, the system **300** includes a smart card/electronic passport **302**, and a terminal module **304**. The smart card/electronic passport may be any one of the smart cards or electronic passports described in the above embodiments. The terminal module **304** includes a terminal module antenna **306**, a decryption circuit **308**, an encryption circuit **310**, and an interface **312**. The decryption circuit **308** is adapted to decrypt signals received from the smart card/electronic passport **302**, if the received signals are encrypted. The encryption circuit **310** encrypts signals transmitted from the terminal module **304**. The interface **312** couples the terminal module **304** to a computer system **314**, typically a local computer network. The interface **312** may also couple the terminal module with a server **316** having a central database **318**. Such a connection to the server **316** may use the Transmission Control Protocol/Internet Protocol (TCP/IP), via a virtual circuit, a private line, or the like. Thus, the interface **312** may be compatible with one of the Universal Serial Bus (USB) standard, Recommended Standard 232C (RS-232C), Recommended Standard 433 (RS-433), Transmission Control Protocol/Internet Protocol (TCP/IP), and the like. The computer system **314** or the server **316** receives the authentication signal and other personal information transmitted from the terminal module **304**, and performs necessary data processing, screening, comparison with the central database, and the like. In addition, the authentication result and/or personal information may be displayed to the authorized personnel.

[0054] Since the electronic passport (or the smart card therein) is powered by the power wirelessly transmitted from the terminal module, as the electronic passport leaves the power range of the terminal module, the supply voltage reduces and eventually shuts

down, turning off the sensor module of the electronic passport. Thus, in accordance with one embodiment of the present invention, the sensor module of the electronic passport (smart card) is automatically initialized in response to a predetermined level of an increasing supply voltage after the supply voltage was shut down. The initialization is typically done by initializing the processor unit of the smart card. If the processor unit includes an authentication CPU and a dual mode interface circuit, for example, the authentication CPU may be initialized using the threshold voltage of the increasing supply voltage, and then the dual mode interface circuit may be initialized using a reset signal supplied from the authentication CPU.

[0055] FIG. 20 schematically illustrates a method for authenticating a person holding a smart card, or an electronic passport embedded with the smart card, in accordance with one embodiment of the present invention. The smart card includes a sensor module provided on a substrate of the smart card, which includes a biometric sensor, a processor unit, and a memory. The smart card or the electronic passport may be any one of the smart cards and electronic passport described above. First, a power signal is received via a wireless transceiver module provided on the substrate (210). This may be such a situation the smart card or passport is placed on a terminal module providing the power signal. At least one supply voltage is generated from the power signal, and the supply voltage is provided to the sensor module (212) so as to power up and enable the sensor module to operate. Optionally, initialization of the sensor module may be performed during the power up period (214). Then, biometric information is detected from the person's body (216), using the biometric sensor, such as a fingerprint sensor, image

sensor, or the like, as described above. The detected biometric information is compared with biometric information stored in the memory (218), and an authentication signal representing a result of the comparing is generated (220). The result of the authentication or comparison is optionally indicated using an indicator provided on the smart card (222). The authentication signal is then optionally encrypted (224) and transmitted via the wireless transceiver module (226).

[0056] While embodiments and applications of this invention have been shown and described, it would be apparent to those skilled in the art having the benefit of this disclosure that many more modifications than mentioned above are possible without departing from the inventive concepts herein. The invention, therefore, is not to be restricted except in the spirit of the appended claims.

CLAIMS

What is claimed is:

1. A smart card for authenticating a person holding said smart card, said smart card comprising:

a substrate;

a sensor module provided on said substrate, said sensor module including:

a biometric sensor adapted to detect biometric information from the person's body;

a processor unit coupled to said biometric sensor, said processor unit adapted to authenticate the person in response to the detected biometric information and generate an authentication signal representing an authentication result; and

a memory coupled to said processor unit, said memory adapted to store biometric information of a specific individual associated with the smart card;

a wireless transceiver module coupled to said processor unit, said wireless transceiver module adapted to transmit signals received from said processor unit and receive a wirelessly-transmitted power signal; and

a power circuit provided on said substrate, said power circuit adapted to generate at least one supply voltage from the received power signal and provide the supply voltage to said sensor module.

2. The smart card of claim 1, wherein said memory includes:

a random access memory (RAM); and

one-time programmable read only memory (PROM).

3. The smart card of claim 2, wherein the one-time PROM includes:
an erasable and programmable read-only memory (EPROM);
an electrically erasable and programmable read-only memory (EEPROM); and
a flash memory,

wherein a rewritable function of the PROM is disabled.

4. The smart card of claim 1, wherein said wireless transceiver module includes:
a power antenna coupled to said power circuit, said power antenna adapted to
receive the power signal; and

a signal antenna coupled to said processor unit, said signal antenna adapted to
transmit signals received from said processor unit.

5. The smart card of claim 4, wherein said signal antenna is substantially smaller
than said power antenna.

6. The smart card of claim 4, wherein said smart card is used with a terminal module
including a module antenna adapted to receive signals from said signal antenna, and
wherein said signal antenna is placed on a proximity position on a loop or trace of the
module antenna.

7. The smart card of claim 4, said power circuit includes:
a rectifier coupled to said power antenna; and
a regulator coupled to said rectifier.
8. The smart card of claim 7, wherein said rectifier includes:
a double voltage rectifier.
9. The smart card of claim 7, wherein said regulator includes one of:
a dropper regulator;
a switching regulator; and
a fly back regulator.
10. The smart card of claim 7, wherein said rectifier includes:
a Shattuck diode.
11. The smart card of claim 4, wherein said wireless transceiver module includes:
a plurality of power antennas,
and wherein said power circuit includes:
a plurality of regulator circuits, each of said regulator circuits coupled to a
corresponding one of the plurality of power antennas.
12. The smart card of claim 11, wherein each of said plurality of power antennas has
a turn number less than 5.

13. The smart card of claim 11, wherein each of said plurality of power antennas has approximately the same length.
14. The smart card of claim 11, wherein said plurality of power antennas are formed as an etched or printed pattern on a plastic or paper material.
15. The smart card of claim 1, wherein said wireless transceiver module is capable of transmitting and receiving electromagnetic waves.
16. The smart card of claim 1, wherein said wireless transceiver module is capable of transmitting and receiving ultrasonic waves.
17. The smart card of claim 1, wherein said wireless transceiver module is capable of transmitting and receiving optical waves.
18. The smart card of claim 1, wherein said wireless transceiver module is capable of transmitting and receiving infrared waves.
19. The smart card of claim 1, wherein said biometric sensor includes:
a fingerprint sensor adapted to detect fingerprint patterns.

20. The smart card of claim 19, wherein said fingerprint sensor is adapted to read the surface profile of a finger.
21. The smart card of claim 20, wherein said fingerprint sensor is adapted to measure the surface profile of finger mechanically, said fingerprint sensor including one of:
- a pressure sensing cell array or scanner;
 - a micro electro mechanical (MEM) array or scanner;
 - a mechanical stress array or scanner;
 - a distance measuring cell array or scanner;
 - an elasticity measuring array or scanner; and
 - a micro switch array or scanner.
22. The smart card of claim 20, wherein said fingerprint sensor is adapted to measure a temperature profile of a skin of a finger.
23. The smart card of claim 22, said fingerprint sensor includes:
- an infrared detector array or scanner.
24. The smart card of claim 20, wherein said fingerprint sensor includes:
- a thinned silicon substrate adapted to detect and digitize fingerprint patterns.
25. The smart card of claim 24, wherein said thinned silicon substrate has a thickness less than about 200 micron.

26. The smart card of claim 25, wherein said thinned silicon substrate is backed up with a mechanical stiffener.
27. The smart card of claim 26, wherein said mechanical stiffener includes a hard polymer.
28. The smart card of claim 19, wherein said biometric information to be stored in said memory includes:
fingerprint templates of the specific individual.
29. The smart card of claim 1, wherein said smart card is flexible.
30. The smart card of claim 29, wherein said biometric sensor comprising:
a polymer material as an insulator, a substrate, or the insulator and substrate.
31. The smart card of claim 30, said polymer material includes at least one of:
polyimide;
polyethylene terephthalate (PET);
Polypropylene (PPT);
Polycarbonate;
Butadiene;
Epoxy;

Nylon;

polymers of tetrafluoroethylene (PTFE); and

polymers of fluorinated ethylene-propylene (FEP).

32. The smart card of claim 1, wherein said biometric sensor includes:
a genetic information detector adapted to detect a genetic information of the person.
33. The smart card of claim 1, wherein said biometric sensor includes:
a charge coupled device (CCD) or metal oxide semiconductor (MOS) adapted to capture an image of the person.
34. The smart card of claim 33, wherein the image of the person includes at least one of:
a face of the person;
an ear of the person;
an iris of the person; and
a retina of the person.
35. The smart card of claim 1, said sensor module further includes:
a biosensor adapted to detect that the person holding the smart card is alive.
36. The smart card of claim 35, wherein said biosensor includes at least one of:

- an oxygen detector;
- a carbon dioxide detector;
- a thermometer;
- a moisture sensor;
- an infrared sensor;
- a voice sensor;
- a brainwave sensor;
- an electrocardiogram sensor;
- an electromagnetic field sensor;
- an enzyme sensor; and
- a Chi sensor.

37. The smart card of claim 35, wherein said biosensor includes at least one of:

- an elasticity sensor adapted to detect elasticity of a member in contact therewith;

and

- a blood flow sensor adapted to detect a blood flow in a body part in contact therewith.

38. The smart card of claim 35, wherein said biosensor includes:

- a bio-response detector adapted to capture a reflex response of the person to a given stimulus.

39. The smart card of claim 38, wherein the reflex response includes:
a change in an iris aperture in response to light intensity illuminated thereon.
40. The smart card of claim 39, wherein said biosensor includes:
an image sensor adapted to capture an image of the iris; and
a light emitter adapted to illuminate an eye of the person.
41. The smart card of claim 1, wherein said sensor module further includes:
an indicator coupled to said processor unit, said indicator adapted to indicate the authentication result.
42. The smart card of claim 41, wherein said indicator includes:
at least one light emitting diode (LED).
43. The smart card of claim 41, wherein said indicator includes:
a liquid crystal display (LCD) adapted to display the authentication result.
44. The smart card of claim 41, wherein said indicator includes:
a sound player adapted to play an audio signal corresponding to the authentication result.
45. The smart card of claim 44, wherein the audio signal has a different frequency depending on the authentication result.

46. The smart card of claim 44, wherein the audio signal has a different voice message depending on the authentication result.
47. The smart card of claim 44, wherein the audio signal has a different melody depending on the authentication result.
48. The smart card of claim 1, wherein said sensor module further includes:
a control interface coupled to said processor unit, said control interface adapted to receive an external control signal and configure said processor unit.
49. The smart card of claim 48, wherein said control interface's connections to the external control signal is disabled after an initial configuration of said processor unit.
50. The smart card of claim 49, wherein said control interface's connections to the external control signal is permanently disabled by a physical disconnection after the initial configuration.
51. The smart card of claim 49, wherein the initial configuration includes writing the biometric information of the specific individual to said memory.
52. The smart card of claim 1, wherein said processor unit includes:
an encryption circuit adapted to encrypt signals generated by said processor unit.

53. The smart card of claim 1, wherein said processor unit includes:
an authentication circuit adapted to compare the detected biometric information with the biometric information stored in said memory, and generate the authentication signal.
54. The smart card of claim 53, wherein said authentication circuit includes:
an authentication program stored in an one-time programmable read only memory (PROM) within said memory.
55. The smart card of claim 54, wherein the one-time PROM includes one of:
an electrically erasable and programmable read-only memory (EEPROM); and
a flash memory,
wherein a rewritable function of the PROM is disabled.
56. The smart card of claim 53, wherein said authentication circuit includes:
an encryption circuit adapted to encrypt the authentication signal.
57. The smart card of claim 53, wherein said authentication circuit is implemented using one of:
hardware;
software;

firmware; and

a combination of at least two of hardware, software, and firmware.

58. The smart card of claim 53, wherein said memory is further adapted to store personal information of the specific individual.

59. The smart card of claim 58, wherein the personal information includes at least one of:

personal identification information; and

personal information related to a purpose or usage of the smart card.

60. The smart card of claim 58, wherein said processor unit further includes:

a retrieval circuit adapted to retrieve the stored personal information from said memory if the detected biometric information is determined to match the stored biometric information.

61. The smart card of claim 60, wherein said processor unit further generates a personal information signal representing the personal information of the specific individual, the personal information signal being transmitted via the wireless transceiver module.

62. The smart card of claim 53, wherein said processor unit further includes:

an interface circuit coupled to said authentication circuit, said interface circuit

adapted to convert a signal received from authentication unit into a signal suitable for wireless transmission.

63. The smart card of claim 62, wherein said interface circuit includes:
- a decryption circuit adapted to decrypt an encrypted signal received from said authentication circuit; and
 - an encryption circuit adapted to encrypt a signal to be wirelessly transmitted.
64. The smart card of claim 1, further comprising:
- an oscillation circuit adapted to generate a clock signal for said sensor module.
65. The smart card of claim 1, further comprising:
- a clock antenna adapted to receive the power signal; and
 - a clock circuit coupled to said clock antenna, said clock circuit adapted to generate a clock signal from the received power signal.
66. The smart card of claim 1, wherein said biometric sensor is located near an edge of said smart card.
67. The smart card of claim 1, wherein said smart card is adapted to be embedded in a passport.

68. The smart card of claim 1, wherein said smart card is a card-type electronic passport.

69. The smart card of claim 68, further comprising:

a card surface layer provided on said substrate, said biometric sensor being visibly arranged on said card surface layer, said card surface layer containing desired information related to the passport.

70. The smart card of claim 1, further comprising:

a display provided on said substrate, said display coupled to said processor unit, said display adapted to display a photographic image including the specific individual's face if the person is authenticated.

71. The smart card of claim 70, wherein said display is further adapted to display a signature of the specific individual if the person is authenticated.

72. The smart card of claim 70, wherein said display is activated by the authentication signal representing a positive result.

73. The smart card of claim 70, wherein said biometric sensor and said display are integrated.

74. The smart card of claim 73, wherein said biometric sensor is substantially transparent and laid on said display.

75. A passport comprising a smart card therein, said smart card including:

a substrate;

a sensor module provided on said substrate, said sensor module including:

a biometric sensor adapted to detect biometric information from a person's body;

a processor unit coupled to said biometric sensor, said processor unit adapted to authenticate the person in response to the detected biometric information and generate an authentication signal representing an authentication result; and

a memory coupled to said processor unit, said memory adapted to store biometric information of a specific individual associated with the smart card;

a wireless transceiver module coupled to said processor unit, said wireless transceiver module adapted to transmit signals received from said processor unit and receive a wirelessly-transmitted power signal; and

a power circuit provided on said substrate, said power circuit adapted to generate at least one supply voltage from the received power signal and provide the supply voltage to said sensor module.

76. The passport of claim 75, wherein said wireless transceiver module includes:

a power antenna coupled to said power circuit, said power antenna adapted to receive the power signal; and

a signal antenna coupled to said processor unit, said signal antenna adapted to transmit signals received from said processor unit.

77. The passport of claim 76, wherein said power circuit includes:

a power circuit coupled to said power antenna, said power circuit adapted to generate at least one supply voltage.

78. The passport of claim 76, wherein said signal antenna is substantially smaller than said power antenna.

79. The passport of claim 76, wherein said wireless transceiver module includes:

a plurality of power antennas,
and wherein said power circuit includes:

a plurality of regulator circuits, each of said regulator circuits coupled to a corresponding one of the plurality of antennas.

80. The passport of claim 79, wherein each of said plurality of power antennas has a turn number less than 5.

81. The passport of claim 79, wherein each of said plurality of power antennas has approximately the same length.

82. The passport of claim 79, wherein said plurality of power antennas are formed as an etched or printed pattern on a plastic or paper material.

83. The passport of claim 75, wherein said wireless transceiver module is capable of transmitting and receiving electromagnetic waves.

84. The passport of claim 75, wherein said wireless transceiver module is capable of transmitting and receiving ultrasonic waves.

85. The passport of claim 75, wherein said wireless transceiver module is capable of transmitting and receiving optical waves.

86. The passport of claim 75, wherein said wireless transceiver module is capable of transmitting and receiving infrared waves.

87. The passport of claim 75, wherein said biometric sensor includes:
a fingerprint sensor for detecting fingerprint patterns.

88. The passport of claim 87, wherein said biometric information to be stored in said memory includes:
fingerprint templates of the specific individual.

89. The passport of claim 75, wherein said biometric sensor includes:
a genetic information detector adapted to detect a genetic information of the person.
90. The passport of claim 75, wherein said biometric sensor includes:
a charge coupled device (CCD) or a metal oxide semiconductor (MOS) adapted to capture an image of the person.
91. The passport of claim 90, wherein the image of the person includes at least one of:
a face of the person;
an ear of the person;
an iris of the person; and
a retina of the person.
92. The passport of claim 75, said sensor module further includes:
a biosensor adapted to detect that the person holding the smart card is alive.
93. The passport of claim 92, wherein said biosensor includes at least one of:
an oxygen detector;
a carbon dioxide detector;
a thermometer;
a moisture sensor; and
an infrared sensor.

94. The passport of claim 92, wherein said biosensor includes at least one of:
an elasticity sensor adapted to detect elasticity of a member in contact therewith;
and
a blood flow sensor adapted to detect a blood flow in a body part in contact therewith.
95. The passport of claim 92, wherein said biosensor includes:
a bio-response detector adapted to capture a reflex response of the person to a given stimulus.
96. The passport of claim 95, wherein the reflex response includes:
a change in an iris aperture in response to light intensity illuminated thereon.
97. The passport of claim 96, wherein said biosensor includes:
an image sensor adapted to capture an image of the iris; and
a light emitter adapted to illuminate an eye of the person.
98. The passport of claim 75, wherein said sensor module further includes:
an indicator coupled to said processor unit, said indicator adapted to indicate the authentication result.

99. The passport of claim 98, wherein said indicator includes:
at least one light emitting diode (LED).
100. The passport of claim 98, wherein said indicator includes:
a liquid crystal display (LCD) adapted to display the authentication result.
101. The passport of claim 98, wherein said indicator includes:
a sound player adapted to play an audio signal corresponding to the authentication result.
102. The passport of claim 101, wherein the audio signal has a different frequency depending on the authentication result.
103. The passport of claim 101, wherein the audio signal has a different voice message depending on the authentication result.
104. The passport of claim 101, wherein the audio signal has a different melody depending on the authentication result.
105. The passport of claim 75, wherein said sensor module further includes:
a control interface coupled to said processor unit, said control interface adapted to receive an external control signal and configure said processor unit.

106. The passport of claim 105, wherein said control interface's connections to the external control signal is disabled after an initial configuration of said processor unit.

107. The passport of claim 106, wherein said control interface's connections to the external control signal is permanently disabled by a physical disconnection after the initial configuration.

108. The passport of claim 106, wherein the initial configuration includes writing the biometric information of the specific individual to said memory.

109. The passport of claim 75, wherein said processor unit includes:
an encryption circuit adapted to encrypt signals generated by said processor unit.

110. The passport of claim 75, wherein said processor unit includes:
an authentication circuit adapted to compare the detected biometric information with the biometric information stored in said memory, and generate the authentication signal.

111. The passport of claim 110, wherein said authentication circuit includes:
an encryption circuit adapted to encrypt the authentication signal.

112. The passport of claim 110, wherein said authentication circuit is implemented using one of:

hardware;
software; and
a combination of hardware and software.

113. The passport of claim 110, wherein said memory is further adapted to store personal information of the specific individual.

114. The passport of claim 113, wherein the personal information includes at least one of:

personal identification information; and
personal information related to a purpose or usage of the smart card.

115. The passport of claim 113, wherein said processor unit further includes:
a retrieval circuit adapted to retrieve the stored personal information from said memory if the detected biometric information is determined to match the stored biometric information.

116. The passport of claim 115, wherein said processor unit further generates a personal information signal representing the personal information of the specific individual, the personal information signal being transmitted via the signal antenna.

117. The passport of claim 110, wherein said processor unit further includes:
an interface circuit coupled to said authentication circuit, said interface circuit

adapted to convert a signal received from authentication unit into a signal suitable for wireless transmission.

118. The passport of claim 117, wherein said interface circuit includes:

a decryption circuit adapted to decrypt an encrypted signal received from said authentication circuit; and

an encryption circuit adapted to encrypt a signal to be wirelessly transmitted.

119. The passport of claim 75, further comprising:

an oscillation circuit adapted to generate a clock signal for said sensor module.

120. The passport of claim 75, further comprising:

a clock antenna adapted to receive the power signal; and

a clock circuit coupled to said clock antenna, said clock circuit adapted to generate a clock signal from the received power signal.

121. The passport of claim 75, wherein said biometric sensor is located near an edge of said smart card.

122. The passport of claim 75, wherein said smart card is embedded in a front or back cover of the passport such that said biometric sensor is visibly arranged on an inner side of the front or back cover.

123. The passport of claim 122, wherein said biometric sensor is placed on the inner side such that said biometric sensor does not interfere with the specific individual's photograph and personal data on the inner side.

124. The passport of claim 122, wherein said indicator is also visibly arranged on the inner side of the front or back cover.

125. The passport of claim 124, wherein said biometric sensor and said indicator are placed on the inner side such that said biometric sensor and said indicator do not interfere with the specific individual's photograph and personal data on the inner side.

126. The passport of claim 122, wherein said smart card further includes:
a display coupled to said processor unit, said display adapted to display a photographic image including the specific individual's face if the person is authenticated, said display being visibly arranged on the inner side of the front or back cover of said passport.

127. The passport of claim 126, wherein said display is further adapted to display a signature of the specific individual if the person is authenticated.

128. The passport of claim 126, wherein said display is activated by the authentication signal representing a positive result.

129. The passport of claim 126, wherein said biometric sensor and said display are integrated.

130. The passport of claim 129, wherein said biometric sensor is substantially transparent and laid on said display.

131. A method for authenticating a person holding a smart card, the smart card including a sensor module provided on a substrate of the smart card, the sensor module including a biometric sensor, a processor unit, and a memory, said method comprising:

receiving a power signal via a wireless transceiver module provided on the substrate;

generating at least one supply voltage from the power signal and supplying the supply voltage to the sensor module;

detecting, by the biometric sensor, biometric information from the person's body; comparing the detected biometric information and biometric information stored in the memory;

generating an authentication signal representing a result of said comparing; and

transmitting the authentication signal via the wireless transceiver module.

132. The method of claim 131, wherein the sensor module further includes an indicator, said method further comprising:

indicating the result of said comparing by the indicator.

133. The method of claim 132, wherein said indicating includes:
indicating the result using at least one light emitting diode (LED).
134. The method of claim 132, wherein said indicating includes:
displaying the result using a liquid crystal display (LCD).
135. The method of claim 132, wherein said indicating includes:
playing a audio signal representing the result.
136. The method of claim 135, wherein the audio signal has a different frequency
depending on the result.
137. The method of claim 135, wherein the audio signal has a different voice message
depending on the result.
138. The method of claim 135, wherein the audio signal has a different melody
depending on the result.
139. The method of claim 131, wherein said detecting includes:
detecting fingerprint patterns of the person.

140. The method of claim 139, wherein said comparing includes:
comparing the fingerprint patterns with fingerprint templates stored in the memory.
141. The method of claim 131, wherein said detecting includes:
capture an image of the person,
wherein the image including at least one of:
a face of the person;
an ear of the person;
an iris of the person; and
a retina of the person.
142. The method of claim 131, further comprising:
detecting, by a biosensor, that the person holding the smart card is alive.
143. The method of claim 142, wherein said detecting includes at least one of:
detecting oxygen;
detecting carbon dioxide;
detecting a temperature;
detecting moisture; and
detecting an infrared radiation.

144. The method of claim 142, wherein said detecting includes at least one of:
detecting elasticity of a member in contact with the biosensor;
detecting a blood flow in a body part in contact with the biosensor;
145. The method of claim 142, wherein said detecting includes:
capturing a reflex response of the person to a given stimulus.
146. The method of claim 145, wherein the reflex response includes:
a change in an iris aperture in response to light intensity illuminated thereon.
147. The method of claim 146, further comprising:
illuminating an eye of the person.
148. The method of claim 131, further comprising:
supplying an external control signal via a control interface so as to configure the sensor module;
supplying, via the control interface, biometric information of a specific individual associated with the smart card, and storing the biometric information in the memory; and
disabling connections to the control interface after said supplying the external control and said storing the biometric information in the memory.
149. The method of claim 148, wherein said disabling includes:
physically disconnecting external access to the control interface.

150. The method of claim 148, further comprising:
storing in the memory personal information of the specific individual.
151. The method of claim 150, wherein said personal information includes at least one of:
personal identification information; and
personal information related to a purpose or usage of the smart card.
152. The method of claim 150, further comprising:
retrieving the stored personal information from the memory if the detected biometric information is determined to match the biometric information template;
generating a personal information signal representing the retrieved personal information; and
transmitting the personal information signal via the wireless transceiver module.
153. The method of claim 131, further comprising:
generating a clock signal for the sensor module using an oscillation circuit provided on the smart card.
154. The method of claim 131, further comprising:
generating a clock signal for the sensor module using the power signal.

155. The method of claim 131, wherein the smart card is embedded in a passport, and the specific individual associate with the smart card is a person to which the passport is issued.

156. The method of claim 131, further comprising:
initializing the sensor module in response to a predetermined level of an increasing supply voltage after the supply voltage was shut down.

157. The method of claim 131, further comprising:
encrypting the authentication signal.

158. The method of claim 157, further comprising:
decrypting the encrypted authentication signal;
converting the decrypted authentication signal into a transmission signal for wireless transmission; and
encrypting the transmission signal.

159. An apparatus for authenticating a person holding a passport, said apparatus comprising:
means for supporting other means thereon, adapted to be embedded in a passport;
means for storing biometric information of a specific individual associated with the passport;

means for detecting biometric information from the person's body;

means for authenticating the person in response to the detected biometric information and for generating an authentication signal representing an authentication result;

means for wirelessly transmitting signals received from said means for authenticating;

means for receiving a wirelessly-transmitted power signal; and

means for generating from the received power signal a supply voltage for other means.

160. The apparatus of claim 159, wherein said means for authenticating includes:

means for comparing the detected biometric information with the stored biometric information.

161. The apparatus of claim 159, wherein the sensor module further includes:

means for indicating the authentication result.

162. The apparatus of claim 161, wherein said means for indicating includes:

at least one light emitting diode (LED).

163. The apparatus of claim 161, wherein said means for indicating includes:

means for displaying the result using a liquid crystal display (LCD).

164. The apparatus of claim 161, wherein said means for indicating includes:
means for playing an audio signal representing the result.
165. The apparatus of claim 164, wherein the audio signal has a different frequency depending on the result.
166. The apparatus of claim 164, wherein the audio signal has a different voice message depending on the result.
167. The apparatus of claim 164, wherein the audio signal has a different melody depending on the result.
168. The apparatus of claim 159, wherein said means for detecting includes:
means for detecting fingerprint patterns of the person.
169. The apparatus of claim 168, wherein said means for authenticating includes:
means for comparing the fingerprint patterns with fingerprint templates stored in said means for storing.
170. The apparatus of claim 159, wherein said means for detecting includes:
means for capturing an image of the person,
wherein the image including at least one of:
a face of the person;

an ear of the person;
an iris of the person; and
a retina of the person.

171. The apparatus of claim 159, further comprising:

means for detecting if the person holding the smart card is alive.

172. The apparatus of claim 171, wherein said means for detecting if the person is alive includes at least one of:

means for detecting oxygen;
means for detecting carbon dioxide;
means for detecting a temperature;
means for detecting moisture; and
means for detecting an infrared radiation.

173. The apparatus of claim 171, wherein said means for detecting if the person is alive includes at least one of:

means for detecting elasticity of a member in contact with the biosensor;
means for detecting a blood flow in a body part in contact with the biosensor;

174. The apparatus of claim 171, wherein said means for detecting if the person is alive includes at least one of:

means for capturing a reflex response of the person to a given stimulus.

175. The apparatus of claim 174, wherein the reflex response includes:
a change in an iris aperture in response to light intensity illuminated thereon.
176. The apparatus of claim 175, further comprising:
means for illuminating an eye of the person.
177. The apparatus of claim 159, further comprising:
means for supplying an external control signal via a control interface so as to
configure the sensor module;
means for supplying, via the control interface, biometric information of a specific
individual associated with the smart card, and for writing the biometric information in
said means for storing; and
means for disabling connections to the control interface after supplying the
external control and writing the biometric information.
178. The apparatus of claim 159, further comprising:
means for storing personal information of the specific individual.
179. The apparatus of claim 178, wherein said personal information includes at least
one of:
personal identification information; and
personal information related to a purpose or usage of the smart card.

180. The apparatus of claim 178, further comprising:
means for retrieving the stored personal information if the detected biometric information is determined to match the biometric information template;
means for generating a personal information signal representing the retrieved personal information, the personal information signal being transmitted via said means for wirelessly transmitting.
181. The apparatus of claim 159, further comprising:
means for generating a clock signal using an oscillation circuit.
182. The apparatus of claim 159, further comprising:
means for generating a clock signal using the received power signal.
183. The apparatus of claim 159, further comprising:
means for initializing said means for authenticating in response to a predetermined level of an increasing supply voltage after the supply voltage was shut down.
184. The apparatus of claim 159, further comprising:
means for encrypting the authentication signal.

185. The apparatus of claim 159, further comprising:

means for decrypting the encrypted authentication signal;

means for converting the decrypted authentication signal into a transmission signal for wireless transmission; and

means for encrypting the transmission signal.

186. A terminal module for authenticating a person holding a smart card, the smart card including a sensor module, a power circuit, and a wireless transceiver module provided on a smart card substrate, said sensor module including a biometric sensor, a processor unit, and a memory, said terminal module comprising:

a support plate adapted to receive the smartcard thereon; and

an antenna provided on said support plate, said antenna adapted to transmit a power to the smart card, the power being to be received by the wireless transceiver module of the smart card, and adapted to receive a signal transmitted from the wireless transceiver module of the smart card.

187. The terminal module of claim 186, wherein the wireless transceiver module of the smart card includes a power receiver antenna and a signal transmission antenna, and

wherein said antenna is provided on said support plate such that when the smart card is placed on said support plate the signal transmission antenna substantially aligns on said antenna.

188. The terminal module of claim 186, further comprising:
a decryption circuit adapted to decrypt signals received from the smart card.
189. The terminal module of claim 186, further comprising:
an interface to a computer system.
190. The terminal module of claim 186, wherein said interface is compatible with at least one of:
Universal Serial Bus (USB) standard;
Recommended Standard 232C (RS-232C);
Recommended Standard 433 (RS-433); and
Transmission Control Protocol/Internet Protocol (TCP/IP).
191. The terminal module of claim 186, wherein said antenna includes:
a power transmission antenna; and
a signal receiver antenna.
192. The terminal module of claim 186, wherein the smart card is embedded in a passport, and said support plate has a size suitable to receive the passport.
193. A system for authenticating a person holding a passport, said system comprising:
a smart card embedded in the passport, said smart card including:
a substrate;

a sensor module provided on said substrate, said sensor module including:

- a biometric sensor adapted to detect biometric information from the person's body;
- a processor unit coupled to said biometric sensor, said processor unit adapted to authenticate the person in response to the detected biometric information and generate an authentication signal representing an authentication result; and
- a memory coupled to said processor unit, said memory adapted to store biometric information of a specific individual associated with the smart card;
- a wireless transceiver module coupled to said processor unit, said wireless transceiver module adapted to transmit signals received from said processor unit and receive a wirelessly-transmitted power signal; and
- a power circuit provided on said substrate, said power circuit adapted to generate a supply voltage from the received power signal and provide a supply voltage to said sensor module; and
- a terminal module, including:
 - a support plate adapted to receive the smartcard thereon; and
 - an antenna provided on said support plate, said antenna adapted to transmit a power signal to the smart card, and receive a signal transmitted from the wireless transceiver module of the smart card.

194. The system of claim 193, wherein said wireless transceiver includes:
- a power antenna coupled to said power circuit; and
 - a signal antenna couple to said processor unit.
195. The system of claim 194, wherein said signal antenna is placed on a proximity position on a loop or trace of said antenna of said terminal module when the smart card is placed on said terminal module.