Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2527836 C 2011/02/15

(11)(21) 2 527 836

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2004/06/01
(87) Date publication PCT/PCT Publication Date: 2004/12/16
(45) Date de délivrance/Issue Date: 2011/02/15
(85) Entrée phase nationale/National Entry: 2005/11/30
(86) N° demande PCT/PCT Application No.: US 2004/017272
(87) N° publication PCT/PCT Publication No.: 2004/109455
(30) Priorité/Priority: 2003/05/30 (US60/474,750)

(51) Cl.Int./Int.Cl. *G06F 21/24* (2006.01), *G06F 1/14* (2006.01), *G06F 7/58* (2006.01), *H04L 9/00* (2006.01), *H04L 9/32* (2006.01)

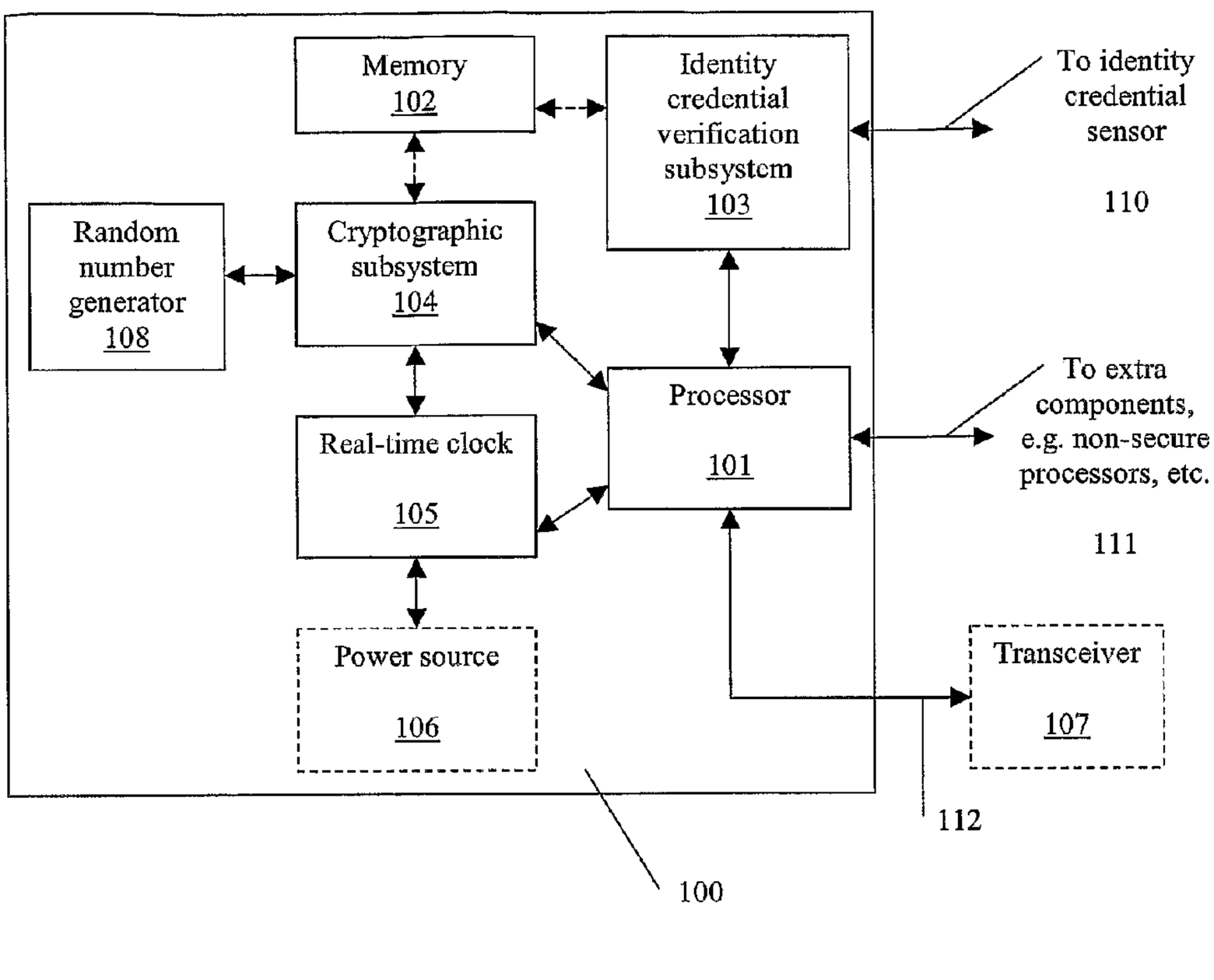
(72) Inventeurs/Inventors:
JOHNSON, BARRY W., US;
TILLACK, JONATHAN A., US;
OLVERA, KRISTEN R., US;
RUSSELL, DAVID R., US

(73) Propriétaire/Owner:
PRIVARIS, INC., US

(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : SYSTEME DE SECURITE EN-CIRCUIT ET PROCEDES DE COMMANDE D'ACCES A ET D'UTILISATION DE DONNEES SENSIBLES

(54) Title: AN IN-CIRCUIT SECURITY SYSTEM AND METHODS FOR CONTROLLING ACCESS TO AND USE OF SENSITIVE DATA



(57) Abrégé/Abstract:
The invention disclosed herein is an in-circuit security system (100) for electronic devices. The in-circuit security system (100) incorporates identity credential verification (103), secure data and instruction storage, and secure data transmission capabilities. It comprises a single semiconductor chip, and is secured using industry-established mechanisms for preventing information tampering or eavesdropping, such as the addition of oxygen reactive layers. This invention also incorporates means for establishing security settings, profiles, and responses for the in-circuit security system (100) and enrolled individuals. The in-circuit security system (100) can be used in a variety of electronic devices, including handheld computers, secure facility keys, vehicle operation/ignition systems, and digital rights management.

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

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 December 2004 (16.12.2004)

PCT

(10) International Publication Number
WO 2004/109455 A3

(51) International Patent Classification[7]: H04L 9/00, 9/32, G06F 12/14

(21) International Application Number: PCT/US2004/017272

(22) International Filing Date: 1 June 2004 (01.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/474,750 30 May 2003 (30.05.2003) US

(71) Applicant: **PRIVARIS, INC.** [US/US]; 675 Peter Jefferson Parkway, Suite 150, Charlottesville, VA 22911 (US).

(72) Inventors: **JOHNSON, Barry, W.**; 1413 Teakwood Cove, Charlottesville, VA 22911 (US). **TILLACK, Jonathan, A.**; 115 Wood Duck Place #404, Charlottesville, VA 22902 (US). **OLVERA, Kristen, R.**; 1642 Center Avenue, Charlottesville, VA 22903 (US). **RUSSELL, David, R.**; P.O. Box 913, Virginia Beach, VA 23451-0913 (US).

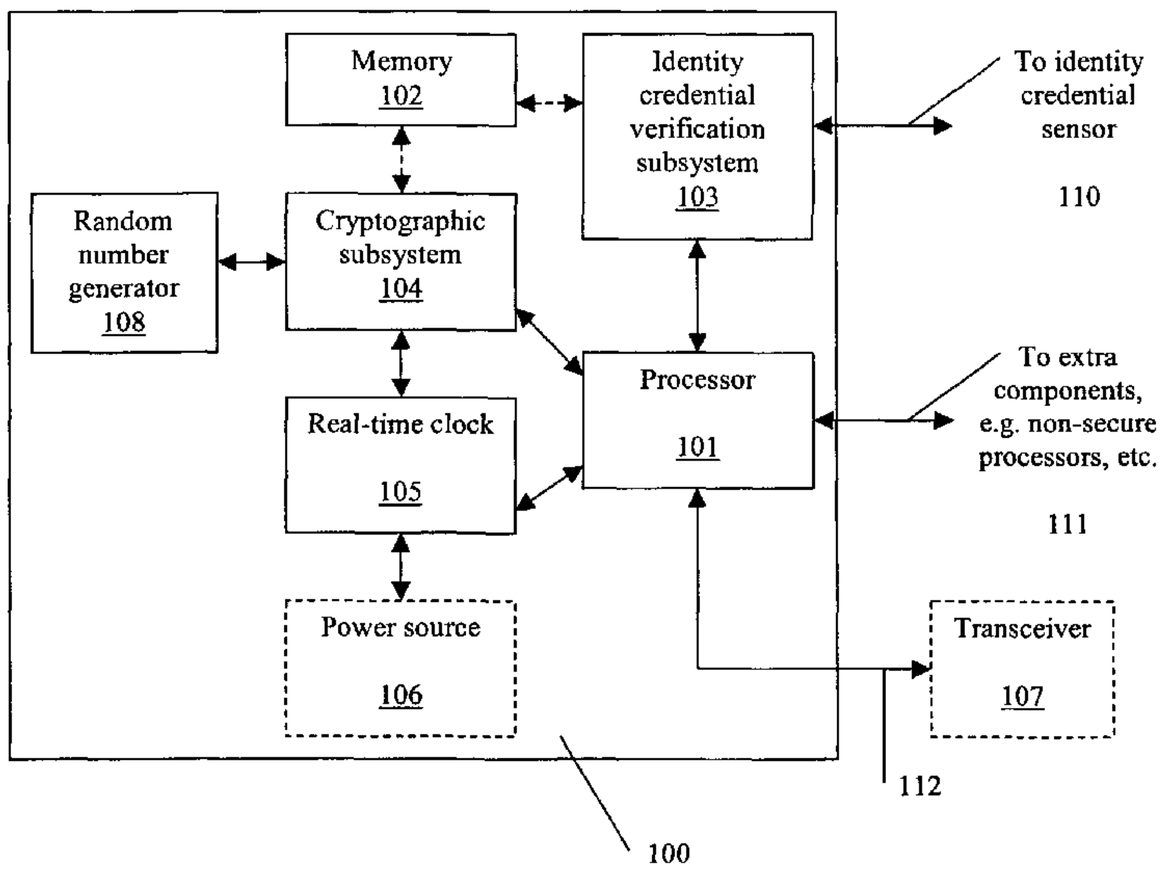
(74) Agents: **CHASTEEN, Kimberly, A.** et al.; Williams Mullen, Fountain Plaza Three, 721 Lakefront Commons, Newport News, VA 23606 (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI,

[Continued on next page]

(54) Title: AN IN-CIRCUIT SECURITY SYSTEM AND METHODS FOR CONTROLLING ACCESS TO AND USE OF SENSITIVE DATA



(57) Abstract: The invention disclosed herein is an in-circuit security system (100) for electronic devices. The in-circuit security system (100) incorporates identity credential verification (103), secure data and instruction storage, and secure data transmission capabilities. It comprises a single semiconductor chip, and is secured using industry-established mechanisms for preventing information tampering or eavesdropping, such as the addition of oxygen reactive layers. This invention also incorporates means for establishing security settings, profiles, and responses for the in-circuit security system (100) and enrolled individuals. The in-circuit security system (100) can be used in a variety of electronic devices, including handheld computers, secure facility keys, vehicle operation/ignition systems, and digital rights management.

WO 2004/109455 A3

WO 2004/109455 A3

SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
3 February 2005

(48) Date of publication of this corrected version:
31 March 2005

(15) Information about Correction:
see PCT Gazette No. 13/2005 of 31 March 2005, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TITLE

An In-circuit Security System and Methods for Controlling Access to and Use of Sensitive Data

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION:

[02] The invention disclosed herein relates to the security of sensitive data stored, processed and distributed using electronic circuits. More particularly, the invention relates to the identification of individuals prior to accessing/using data, and the execution of security controls upon unauthorized attempts to access/use said data.

[03] In recent years there has been an explosion of electronic devices that individuals may use for storing and transmitting sensitive data. In a low-security example, portable devices like a Palm™ or BlackBerry handheld computer typically contain software for e-mail, along with options for storing credit cards, schedules, and other data. Most people wish to protect this information, but most handheld devices rely on their operating system to secure data. Unfortunately, the most common operating systems for these handheld computers were not designed with security as the main goal, and retrofitting basic security mechanisms has been clumsy.

[04] A growing number of electronic devices, such as smart cards, are intended to specifically identify and authenticate users using the public key infrastructure, which requires

secure storage of private keys. These devices are common in building security; for example, an individual with proper authorization to access a facility is assigned a smart card and an asymmetric key pair. A certificate authority generates a digital certificate for the public key, which is stored in the smart card. The private key is also stored on the smart card. When the individual places his smart card in the reader at the access point of the facility, the card transmits its digital certificate, and the reader challenges the card to encrypt a supplied string with the individual's private key. The reader obtains the public key out of the digital certificate and decrypts the private key-encrypted string to verify that the keys are related. This has an inherent problem because there is no guarantee that the individual using the private key is the assigned owner of the smart card. Furthermore, it is fairly simple for an experienced attacker to gain access to keys stored on the card.

[05] Some handheld devices, such as Hewlett Packard's iPAQ PocketPC h5450, include biometric sensors for improved personal identification before allowing access to sensitive data. An individual possessing this device is instructed to enroll one or more of his fingerprints into the device's software. The enrolled fingerprint can be used as the sole password or as an alternative to a typed password. This type of device can be a substantial improvement on traditional data-access methods, because the biometric can be definitively tied to a single individual. However, if the sensitive data is stored or transmitted insecurely, the biometric authentication does not substantially hinder an attacker from probing the memory and compromising it.

[06] These concerns have contributed to the marketing of products billed as 'secure memory' or 'secure processor'. These products are typically constructed with varying degrees of security; one lower degree is considered 'tamper-evident', in which an unskilled observer would see that someone had attempted to maliciously gain access to secured data. A higher level is 'tamper-resistant', in which the product actively resists tampering by use of a

self-destruct mechanism, an impermeable substance that coats the components storing sensitive data such as a polymer-based coating or other so-called "conformal coating", or some other process. Furthermore, these products may encrypt input/output lines, mislabel parts, and perform other types of obfuscation.

Description of the Related Art:

[07] U.S. Patent No. 5,533,123 to Force, et al., discloses programmable distributed personal security inventions. The patent teaches a "Secured Processing Unit" ('SPU') comprising an "SPU chip" and a microprocessor designed especially for secure data processing. The invention integrates keys, encryption and decryption engines, and algorithms in the SPU of the invention. Purportedly, the security process is portable and easily distributed across physical boundaries. The invention is based upon three interdependent subsystems. The first subsystem of the invention is a detector subsystem, which alerts an SPU to the existence and to the character of a security attack. A second subsystem is a filter subsystem that correlates data from multiple detectors, then assesses the severity of the attack against the risk to the SPU's integrity, both to its secret data and to the design of the SPU itself. A third subsystem is a response subsystem for generating responses, or countermeasures, calculated by the filters to be most appropriate under the circumstances, in order to deal with the attack(s) detected. Force does not disclose identity credential verification within the SPU.

[08] U.S. Patent No. 5,825,878 to Takahashi discloses a secure embedded memory management unit for a microprocessor. A microprocessor memory management apparatus is used for encrypted instruction and data transfer from an external memory. Physical security is obtained by embedding the direct memory access controller on the same chip with a microprocessor core, an internal memory, and encryption/decryption logic. Data transfer to and from an external memory takes place between the external memory and the memory

controller of the memory management unit. All firmware to and from the external memory is handled on a page-by-page basis. Since all of the processing takes place on buses internal to the chip, detection of clear unencrypted instructions and data is prevented. Takahashi does not disclose any capability, anticipation, intention, or provision for including identity credential verification on the management unit or within the microprocessor core.

[09] U.S. Patent No. 5,832,207 to Little, et al., teaches a secure module including a microprocessor and a co-processor. The electronic module is provided with at least one microprocessor and a co-processor deployed into a single integrated circuit. The electronic module can be contained in a small form factor housing. The electronic module provides secure bi-directional data communication via a data bus. The electronic module may include an integrated circuit including a microprocessor and a co-processor adapted to handle 1,024-bit modulo mathematics primarily aimed at RSA calculations. The electronic module is preferably contained in a small token-sized metallic container. The module preferably communicates via a single wire data bus using a one-wire protocol. Little et al. does not disclose personal identification systems.

[10] U.S. Patent No. 5,894,550 to Thireit discloses a method of implementing a secure program in a microprocessor card, and a microprocessor card including a secure program. The invention claims that a program can be made secure relative to a CPU. The invention accomplishes this by storing in a first memory zone predetermined address functions that are directly executable by the CPU. The first memory zone is then write-protected, then the program is stored in a second memory zone in the form of a series of instructions that are executable within the second memory zone or that activate functions contained in the first memory zone.

[11] U.S. Patent Nos. 5,481,265, 5,729,220, 6,201,484 and 6,441,770 to Russell detail a handheld device used to authenticate persons and said device to remote computer systems.

The invention further includes a "kill switch" or "kill signal" enabling the computer system to remotely disable the handheld device and restrict further emissions. However, the system is primarily targeted at local area network applications and does not anticipate or suggestion broader applications.

BRIEF SUMMARY OF THE INVENTION

[12] The invention disclosed herein is an in-circuit security system for electronic devices. The in-circuit security system incorporates identity credential verification, secure data and instruction storage, and secure data transmission capabilities. It comprises a single semiconductor chip, lowering component cost and reducing board space. The in-circuit security system chip is secured using mechanisms for preventing information tampering or eavesdropping, such as the addition of oxygen reactive layers. This invention also incorporates means for establishing security settings and profiles for the in-circuit security system and enrolled individuals. The in-circuit security system can be used in a variety of electronic devices, including handheld computers, secure facility keys, vehicle operation/ignition systems, and digital rights management.

BRIEF DESCRIPTION OF DRAWINGS

MASTER REFERENCE NUMERAL LIST

Figure 1: Sample embodiment of in-circuit security system components

100	In-circuit security system
101	Processor
102	Memory
103	Identity credential verification subsystem
104	Cryptographic subsystem
105	Real-time clock
106	Power source (OPTIONAL)
107	Transceiver (OPTIONAL)
108	Random number generator
110	Connection to identity credential sensor
111	Connection to peripheral components
112	Connection to antenna or cables

Figure 2: Handheld computer with the in-circuit security system

100 In-circuit security system
201 Non-secure processor
202 Non-secure memory
203 Fingerprint sensor
204 Antenna
213 Display
214 Keypad

Figure 3: Electronic lock mechanism with the in-circuit security system

100 In-circuit security system
313 LEDs
314 Electronic lock mechanism

[13] FIG. 1 is a schematic view of a sample embodiment of the in-circuit security system.

[14] FIG. 2 is a schematic view of the components of a sample handheld computer using the in-circuit security system.

[15] FIG. 3 is a schematic view of the components of an electronic lock mechanism using the in-circuit security system.

DETAILED DESCRIPTION OF THE INVENTION

[16] The invention described herein is an in-circuit security system by which pre-enrolled individuals may access sensitive data or perform actions on sensitive data in an environment that is fully monitored and protected. The in-circuit security system requires full authentication of individuals and can perform a variety of programmed responses in the event that pre-established authentication standards are not met. The in-circuit security system includes secure transmission of sensitive data to remote devices.

[17] The in-circuit security system comprises several components combined securely into a single, secure chip. As seen in Figure 1, the primary embodiment of the in-circuit security system 100 comprises a processor 101, a memory 102, a real-time clock 105, and a random number generator 108. The in-circuit security system 100 also includes a cryptographic

subsystem 104 and an identity credential verification subsystem 103. These subsystems may be logical, physical, or some combination thereof, and are described in further detail below. In typical embodiments, the in-circuit security system 100 will also contain a power source 106, such as a battery, in order to maintain power to the real-time clock 105. During manufacture, the in-circuit security system 100 receives a unique, one-time programmable electronic identification code that can be read but cannot be altered or removed. The in-circuit security system 100 also preferably provides multiple input/output interfaces 110-112 for connection to optional internal/external components, such as transceivers 107, antennae, identity credential sensors, non-secure processors, etc.

[18] The processor 101 is the main control component; it is responsible for loading and executing instructions to control the various components of the chip, as well as performing user-requested tasks. The memory 102 is coupled to the processor 101. It comprises both volatile and non-volatile components and can be used to store instructions or data, such as security settings or profiles and cryptographic keys. The application of these security settings is discussed below. The real-time clock 105 is also coupled to the processor 101 and is used to maintain an accurate time, which can be used in cryptographic signing, audit records, or other transactions. The real-time clock 105 may be connected to a power source 106 in order to constantly maintain time. If the in-circuit security system 100 does not include the power source 106, the real-time clock 105 must be cognizant of power disconnects, which mean that it can no longer provide an accurate time.

[19] The fourth component of the in-circuit security system 100 is a random number generator 108. The random number generator 108 is used for seeding cryptographic algorithms, and may use any of established methods for guaranteeing sufficient randomness. The random number generator 108 may be included as part of the cryptographic subsystem 104 or may be a standalone component coupled to the subsystem 104. The cryptographic

subsystem 104 is a dedicated system for performing encryption and decryption, digital signing and digital signature verification. In one embodiment the subsystem 104 is responsible for storing cryptographic keys in its own memory; in another, the subsystem is coupled to and uses the main memory 102 of the in-circuit security system 100. Additionally, one primary embodiment of the invention uses a cryptographic acceleration chip or component as the cryptographic subsystem 104. Alternative embodiments are coupled to and use the main processor 101 as the cryptographic engine.

[20] The identity credential verification subsystem 103 is used to determine the identity of an individual attempting to use the in-circuit security system 100 and identify his associated security privileges. The identity credential verification subsystem 103 performs identity credential acquisition, analysis, storage and matching. In the primary embodiment of the invention, the identity credential verification subsystem 103 uses digital representations of fingerprints as the identity credential. In this embodiment the identity credential verification subsystem 103 performs fingerprint image acquisition, and template generation, storage, and matching. The identity credential verification subsystem 103 may use the main processor 101 of the in-circuit security system 100 for credential processing actions or may use its own specialized processor. Similarly, it may employ its own memory for credential storage or use the main memory 102 of the in-circuit security system 100. The in-circuit security system 100 provides one or more connections 110 to external components for credential sensing, such as a fingerprint sensor.

[21] The in-circuit security system 100 incorporates an interface 112 to a transceiver 107, antenna, wire, or other remote communication device that is coupled to the processor 101. This component is used for transmission of data from one device to another. All sensitive data that is to be transmitted from the in-circuit security system 100 can be encrypted using the cryptographic subsystem 104, so it is not necessary to place a transceiver 107 within the

secure boundaries of the in-circuit security system 100. However, in some embodiments it may prove to be convenient to incorporate the transceiver 107 into the chip. In these embodiments the interface 112 would be from the transceiver to an antenna, wire, or other communication device. In a primary embodiment of the invention, the transmission technology is radio-frequency identification (RFID), such as the ISO 14443 A/B or 15693 standards. In another embodiment the in-circuit security system 100 uses Bluetooth or infrared technology. Other embodiments provide a combination of these technologies or others. In alternative embodiments, it may be useful to use a wired technology, such as a serial or USB connection. The in-circuit security system 100 preferably provides external connections 112 for requisite connectors, cables or antennae.

[22] The authentication of individuals allows the in-circuit security system 100 to associate an individual with specific security privileges within the system. For example, one user may be enrolled and identified as a typical user with no ability to reset the system 100, while an alternate user may be identified as an administrator with that ability. Additionally, the in-circuit security system 100 may be programmed to perform a variety of both temporary and permanent responses to security events. For example, a specified number of access denials within a particular time interval may cause the in-circuit security system 100 to suspend all actions or halt the real-time clock 105 until reset by an enrolled administrator. Alternatively, an attempt to crack open the case of the chip housing the in-circuit security system 100 may result in permanent erasure of memory 102, or destruction of other components. The in-circuit security system 100 may also be programmed to allow an enrolled individual to directly disable or destroy components.

[23] As described above, the in-circuit security system 100 is combined into one secured chip with three major interfaces: an interface to a credential sensing mechanism, such as a fingerprint sensor; an interface to peripheral components, such as non-secure processors or

user-interface devices; and an interface to a transceiver or antenna for remote communications. Other interfaces are strictly prevented. The chip may use one or more physical security measures to prevent information eavesdropping. These obfuscation techniques include use of "potting", oxygen-reactive layers, photo-sensors, Hall effect sensors, and circuits that monitor clock frequency and/or reset frequency.

[24] The system 100 may additionally perform algorithmic analysis of interface traffic. For example, fingerprint images received from a fingerprint sensor may be analyzed by the identity credential verification subsystem 103; if the identity credential verification subsystem 103 repeatedly receives the exact same bit pattern representation of fingerprints, it is possible that someone is deliberately placing that bit pattern on the interface. Similarly, if the identity credential verification subsystem 103 receives bit patterns that are an exact rotation or other permutation of a previously received image, again someone may be altering the contents of the interface.

[25] The in-circuit security system can be used as a standalone component for security applications or as one of multiple components within an electronic device. In one use of the invention, a handheld computer is equipped with the in-circuit security system 100, as seen in Figure 2. The computer further comprises a display 213, a keypad 214, a non-secure processor 201 and memory 202, and a fingerprint sensor 203. Additionally, for embodiments in which the in-circuit security system 100 includes a transceiver 107 that uses cellular wireless technology, the handheld computer also incorporates an antenna 204.

[26] The primary user of the handheld computer enrolls a fingerprint, a digital certificate, and an associated private key into the in-circuit security system 100. The fingerprint is stored in the identity credential verification subsystem 103 and is used to authorize use of the private key associated with the digital certificate. The digital certificate may be stored in the cryptographic subsystem 104 or the main memory 102 of the in-circuit security system 100.

[27] The individual typically uses the handheld computer to transmit and receive e-mail. He requires the in-circuit security system 100 to digitally sign his e-mail, which requires accessing the stored private key associated with his fingerprint. He selects his e-mail program, and types an e-mail for transmission using the keypad 214. The keypad 214 is coupled to the processor 201, which receives the data and creates an appropriate message packet for transmission. Once created, the message packet is sent to the in-circuit security system 100 for further processing.

[28] The processor 101 of the in-circuit security system 100 receives the message packet and analyzes the established security settings for transmission of e-mail. Because the in-circuit security system 100 is configured to require digital signing of e-mail prior to transmission, the individual must first authenticate his fingerprint to the identity credential verification subsystem 103. The biometric authentication is required to prevent unauthorized users from encrypting e-mail with a private key that is not theirs. The processor 101 signals the identity credential verification subsystem 103 to wait for a new fingerprint sample from the fingerprint sensor 203, and signals the non-secure processor 201 to provide a visual prompt to the user on the display 213. After the user places his finger on the fingerprint sensor 203 it sends the new fingerprint image to the identity credential verification subsystem 103. The identity credential verification subsystem 103 analyzes the image, generates a template, and compares it to the enrolled fingerprint template. If the two match, the identity credential verification subsystem 103 sends a signal to the processor 101 that the individual is authorized to use the stored private key.

[29] The processor 101 now sends the e-mail message to the cryptographic subsystem 104 and instructs the cryptographic subsystem 104 to sign the message. This typically involves generating a hash of the message and encrypting it with the private key. The cryptographic subsystem 104 may also include a timestamp generated by the real-time clock, the unique

device identifier, or other data, prior to the hash. The cryptographic subsystem 104 now sends the signed e-mail message back to the processor 101. The processor 101, in turn, sends the signed e-mail to the cellular transceiver 107 for transmission to a remote recipient.

[30] In a second embodiment of the invention, the in-circuit security system 100 is embedded into an electronic door locking mechanism that is used to control access to a secure facility. As seen in Figure 3, the system comprises the in-circuit security system 100 with a wired connection to the electronic door lock 314, a fingerprint sensor 203, and a series of light emitting diodes (LEDs) 313 that are used to provide visual feedback to the user. Individuals access the secure facility by demonstrating enrollment of their fingerprint into the in-circuit security system 100. The security settings of the in-circuit security system 100 are configured to shut down the entire locking mechanism on a pre-specified number of failed attempts within a pre-specified time span. This is example of security parameters and settings that are stored within the memory 102.

[31] An enrolled individual wishes to enter the facility. One LED 313 glows green, signaling that the fingerprint sensor 303 is ready. The individual places his finger on the sensor 203, which generates a fingerprint image and sends it to the identity credential verification subsystem 103. The identity credential verification subsystem 103 generates a fingerprint template and compares it to the enrolled fingerprints. The new fingerprint template matches an existing template, so the identity credential verification subsystem 103 sends the individual's unique identifier to the processor 101. The processor 101 accesses the memory 102, which stores security privileges associated with enrolled individuals. The individual who is currently authenticated is authorized to enter the secure facility alone, so the processor 101 sends a signal to the transceiver 107 to trigger the lock 314 to release.

[32] Now an individual who has not been pre-enrolled into the identity credential verification subsystem 103 attempts to enter the secure facility. The individual places his

finger on the fingerprint sensor 203, which sends an image of the fingerprint back to the identity credential verification subsystem 103. The fingerprint is compared to all of the enrolled fingerprints, and no match is found because the individual is not enrolled. The identity credential verification subsystem 103 records the date, time, and other requisite characteristics of the failed access attempt, and flashes a red LED 313 to show that access has been denied. The identity credential verification subsystem 103 also notifies the appropriate process within the processor 101 that an access failure has occurred.

[33] The individual now tries another, un-enrolled finger. The identity credential verification subsystem 103 records the subsequent failure, and notifies the processor 101 that there has been another failure. When the number of failed attempts reaches the pre-established limit, the identity credential verification subsystem 103 again notifies the processor 101 that a failure has occurred. At this point, the processor 101 applies the security settings and places the electronic lock mechanism 314 in a state where it cannot be unlocked unless it is reset by a recognized authority; in a primary embodiment this would be implemented using a "fail-secure" lock and would involve disconnecting a power source. Alternative actions can occur to put the lock 314 into this state as necessary. The processor 101 may also put the identity credential verification subsystem 103 into a state where it does not accept new fingerprints, create images, or perform matching. As desired by the regulator of the secure facility, the processor 101 may instruct the identity credential verification subsystem 103 to delete any enrolled fingerprint images. These are all examples of programmable security settings.

What is claimed is:

1. An in-circuit security system for electronic devices, comprising:

a processor;

a memory, coupled to the processor;

a real-time clock, coupled to the processor;

a cryptographic subsystem, coupled to the processor and the real-time clock;

a random number generator, coupled to the cryptographic subsystem;

an identity credential verification subsystem, coupled to the processor; the processor is configured to halt operation of the real-time clock when the identity credential verification subsystem denies access for a predetermined number within a predetermined period of time;

a power source, coupled to the real-time clock;

at least three input/output interfaces;

wherein, said processor provides means for load and execution of instructions and associated data ;

wherein, said memory provides means for storage of instructions and data, including security settings and profiles;

wherein, said real-time clock provides means for generating an accurate time;

wherein, the power source is configured to provide power to the real-time clock;

wherein, said cryptographic subsystem provides means for performing encryption, decryption, digital signing, and digital signature verification;

wherein, said random number generator provides means for randomly producing a number with statistical randomness sufficient to meet a pre-determined level;

wherein, said identity credential verification subsystem provides means for identity credential acquisition, analysis, storage and matching;

the in-circuit security system excluding the identity credential verification subsystem is disabled until a user is matched based on an acquired identity credential from the user and verified based on the security settings and the profiles for that user;

wherein, a first input/output interface is used for connection between the identity credential verification subsystem and an external identity credential sensor;

wherein, a second input/output interface is used for transmission and receipt of

data to and from a remote connection device; and

wherein, a third input/output line is used for connection to at least one peripheral device.

2. The in-circuit security system of Claim 1, wherein the input/output interface for transmission and receipt of data to and from the remote connection device connects the processor to a transceiver.

3. The in-circuit security system of Claim 2, wherein said transceiver is a wireless communications transceiver.

4. The in-circuit security system of Claim 2, further comprising a connection from said transceiver to an antenna.

5. The in-circuit security system of Claim 2, wherein the transceiver is used for RFID communication.

6. The in-circuit security system of Claim 2, wherein the transceiver is used for Bluetooth communication.

7. The in-circuit security system of Claim 2, wherein the transceiver is used for infrared communication.

8. The in-circuit security system of Claim 1, wherein the input/output interface for transmission and receipt of data to and from a remote connection device connects the processor to a transceiver used for wired communication.

9. The in-circuit security system of Claim 8, wherein the transceiver is used for serial communication.

10. The in-circuit security system of Claim 8, wherein the transceiver is used for USB

communication.

11. The in-circuit security system of Claim 1, wherein the identity credential verification subsystem uses biometric authentication.

12. The in-circuit security system of claim 1, wherein the processor is configured to monitor clock frequency and reset clock frequency.

13. An apparatus, comprising:

a single integrated circuit having

a processor;

a real-time clock coupled to the processor;

a memory coupled to the processor and configured to store an identity credential and a security data associated with the identity credential;

an identity credential verification subsystem coupled to the processor and configured to identify a user based on an identity credential; and

a cryptographic subsystem coupled to the processor and configured to encrypt the security data associated with the identity credential to produce encrypted security data when the identity credential verification subsystem verifies the user,

the processor being configured to halt operation of the real-time clock when the identity credential verification subsystem denies access for a predetermined number within a predetermined period of time,

the single integrated circuit having a first portion associated with a functionality of the identity credential verification subsystem, the single integrated circuit having a second portion not associated with the functionality of the identity credential verification subsystem, the second portion of the single integrated circuit being disabled until the user is identified based on the identity credential and verified based on the security data associated with the identity credential.

14. The apparatus of claim 13, wherein the single integrated circuit further has a random number generator coupled to the cryptographic subsystem and configured to seed a cryptographic algorithm associated with the cryptographic subsystem.

15. The apparatus of claim 13, wherein the cryptographic subsystem is configured to produce a digital signature based on the security data associated with the identity credential.

16. The apparatus of claim 13, further comprising:

a biometric sensor operably coupled to the single integrated circuit, the biometric sensor configured to send biometric data associated with the user to the single integrated circuit,

the identity credential verification subsystem configured to identify the user based on the identity credential and the biometric data.

17. The apparatus of claim 13, further comprising:

a transmitter operably coupled to the single integrated circuit, the transmitter configured to receive the encrypted security data, the transmitter configured to send an authorization signal based on the encrypted security data to a remote device.

18. The apparatus of claim 13, wherein the memory is configured to erase the identity credential and the security data associated with the identity credential when the single integrated circuit is tampered with.

19. The apparatus of claim 13, wherein the single integrated circuit includes a power source coupled to the real-time clock, the power source being configured to provide power to the real-time clock.

20. The apparatus of claim 13, wherein the processor is configured to monitor clock frequency and reset clock frequency.

21. An apparatus, comprising:

a single integrated circuit having

an identity credential verification subsystem configured to identify a user based on an identity credential and user data;

a processor;

a real-time clock coupled to the processor, the processor is configured to halt operation of the real-time clock when the identity credential verification subsystem denies access for a predetermined number within a predetermined period of time;

a cryptographic subsystem configured to encrypt a security data associated with the identity credential to produce encrypted security data when the identity credential verification subsystem verifies the user;

an input/output interface configured to send the encrypted security data from the single integrated circuit; and

a memory configured to erase the identity credential and the security data associated with the identity credential when the single integrated circuit is tampered with,

functionality of the single integrated circuit not used during operation of the identity credential verification subsystem being disabled until the user is identified by the identity credential verification subsystem based on the identity credential.

22. The apparatus of claim 21, wherein the single integrated circuit further has a random number generator coupled to the cryptographic subsystem and configured to seed a cryptographic algorithm associated with the cryptographic subsystem.

23. The apparatus of claim 21, wherein the cryptographic subsystem is configured to produce a digital signature based on the security data associated with the identity credential.

24. The apparatus of claim 21, wherein the user data is biometric data received from a biometric sensor operatively coupled to the single integrated circuit.

25. The apparatus of claim 21, further comprising:

a transmitter operably coupled to the single integrated circuit, the transmitter configured to receive the encrypted security data, the transmitter configured to send an authorization signal based on the encrypted security data to a remote device.

26. The apparatus of claim 21, wherein the single integrated circuit includes a power source,

the real-time clock being configured to produce time,

the power source being coupled to the real-time clock, the power source being configured to provide power to the real-time clock such that the time is constantly maintained by the real-time clock.

27. The apparatus of claim 21, wherein the single integrated circuit is configured to monitor clock frequency and reset clock frequency.

DRAWINGS

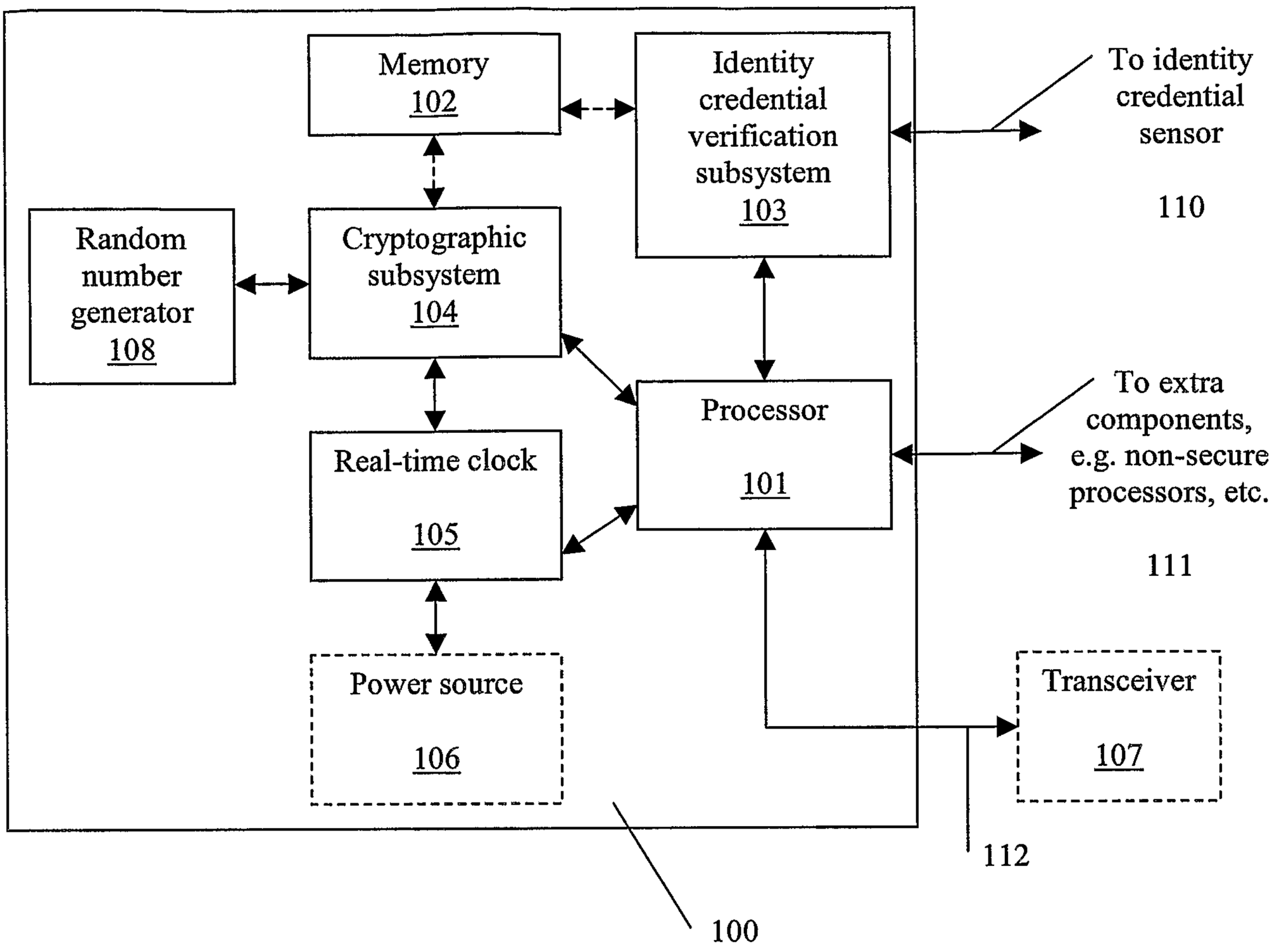


FIGURE 1

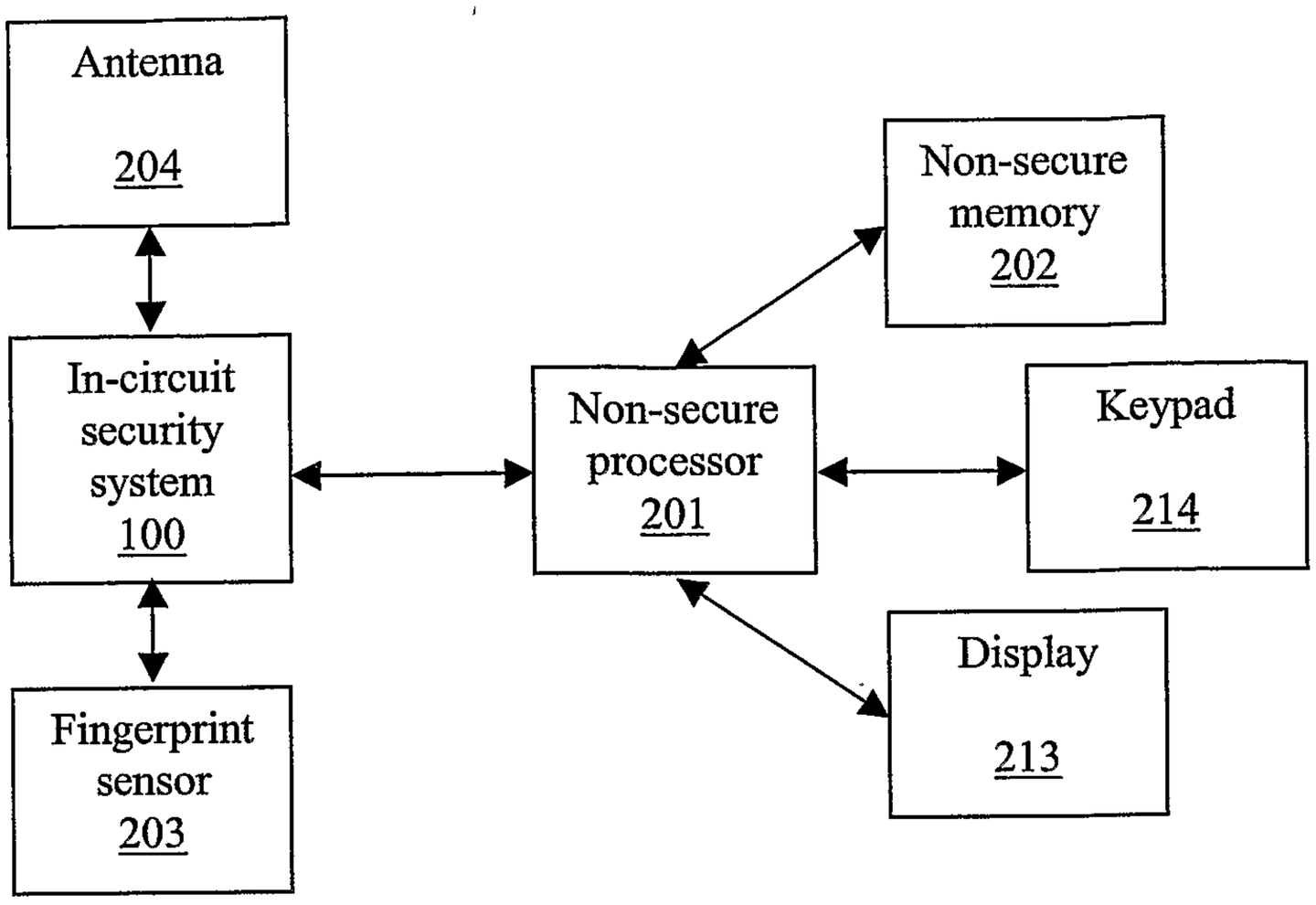


FIGURE 2

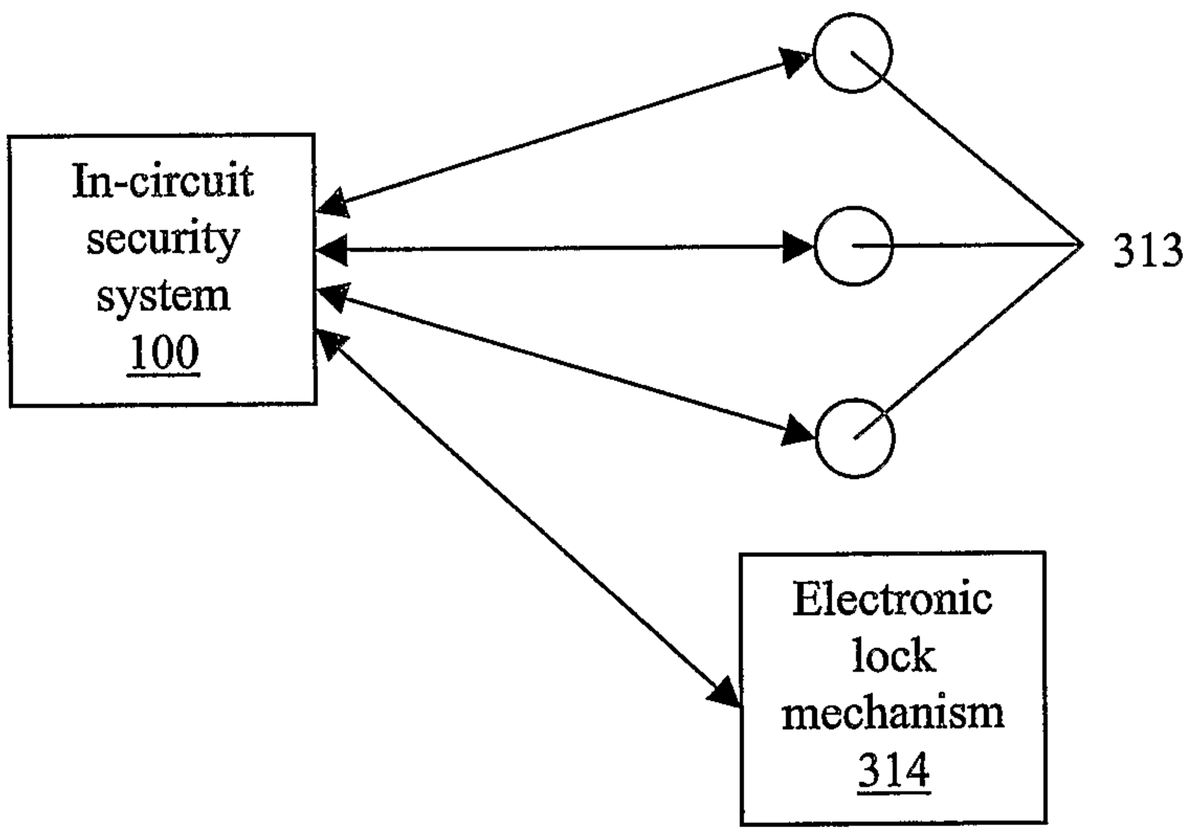
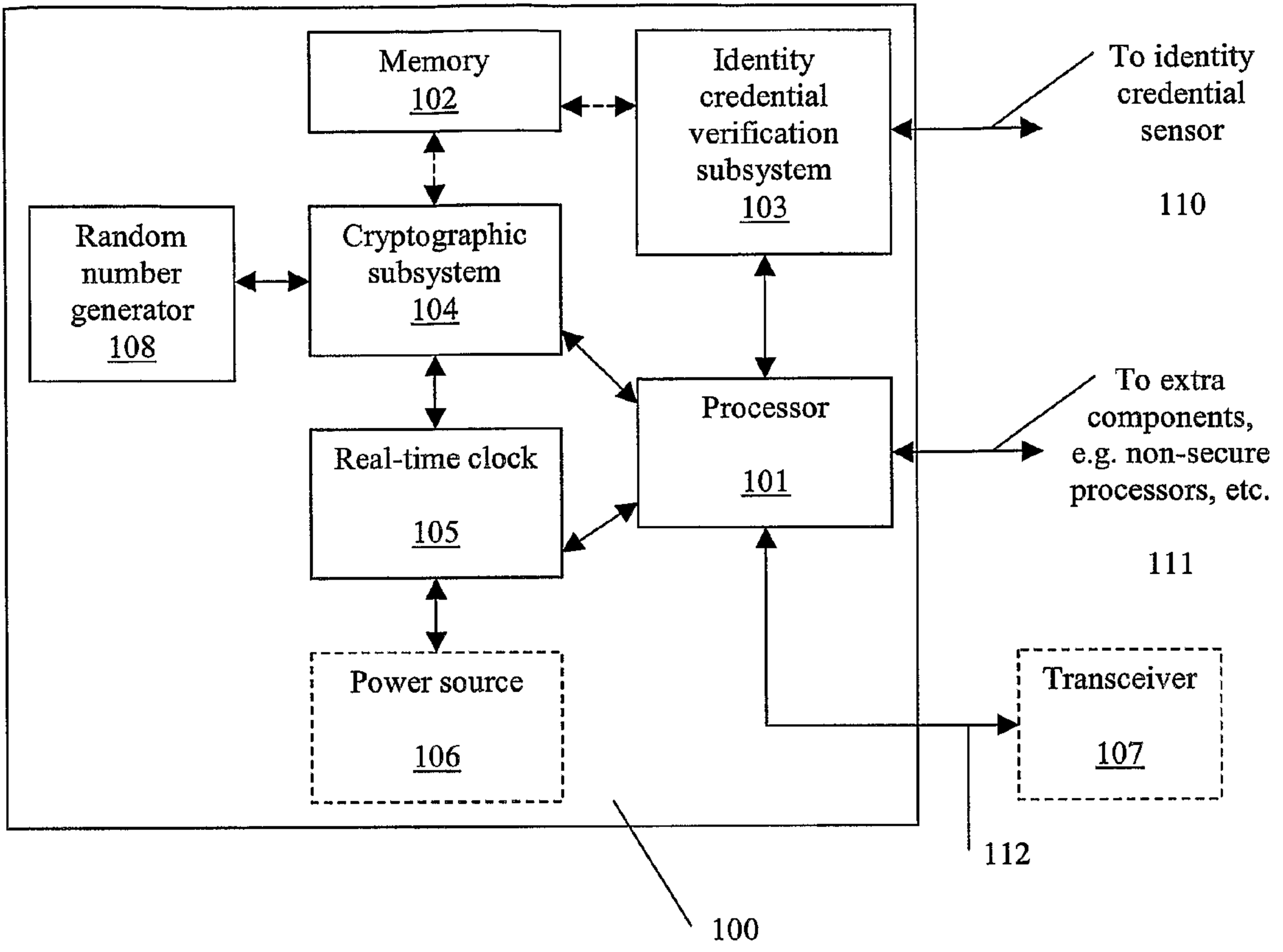


FIGURE 3


Memory
102
Identity credential verification subsystem
103
To identity credential sensor
110
Random number generator
108
Cryptographic subsystem
104
Processor
101
To extra components, e.g. non-secure processors, etc.
111
Real-time clock
105
Power source
106
Transceiver
107
112
100