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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 October 2015 (15.10.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/154185 A1

(51) International Patent Classification:
G06K 19/073 (2006.01) *G06Q 20/40* (2012.01)
G06Q 20/34 (2012.01) *G07C 9/00* (2006.01)

(21) International Application Number:
PCT/CA2015/050286

(22) International Filing Date:
8 April 2015 (08.04.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/249,244 9 April 2014 (09.04.2014) US

(71) Applicant: **CARDEX SYSTEMS INC.** [CA/CA]; 365 Bay Street, Suite 800, Toronto, Ontario M5H 2V1 (CA).

(72) Inventors: **VAN KERREBROECK, Dennis Bernard**; 365 Bay Street, Suite 800, Toronto, Ontario M5H 2V1 (CA). **VAN KERREBROECK, Bernard Marie-Andre**; 365 Bay Street, Suite 800, Toronto, Ontario M5H 2V1 (CA). **HORN, Craig Michael**; 365 Bay Street, Suite 800, Toronto, Ontario M5H 2V1 (CA).

(74) Agent: **ZISCHKA, Matthew**; Smart & Biggar, 438 University Avenue, Box 111, Suite 1500, Toronto, Ontario M5G 2K8 (CA).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SELF-AUTHENTICATING CHIPS

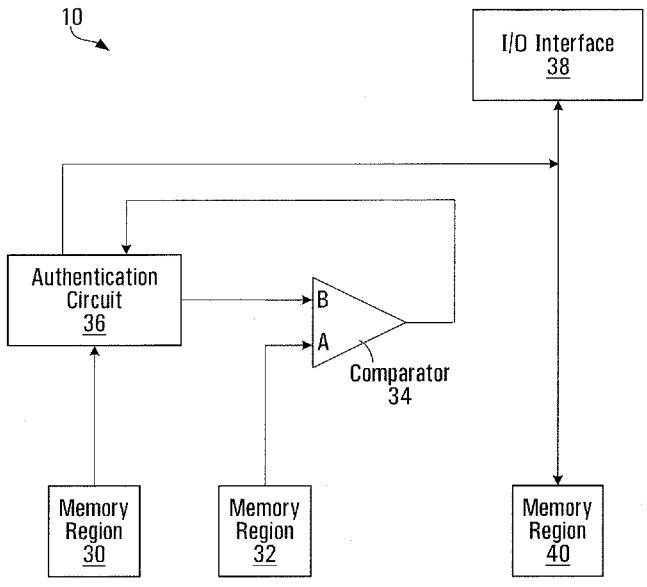


FIG. 4

(57) Abstract: A self-authenticating chip includes first and second memory regions storing, respectively, first and second authentication codes. The second memory region is adapted to be unreadable and unmodifiable by the chip or a chip reader. The chip also includes a comparator for providing an indicator of whether given input matches the second authentication code. The chip also includes an authentication circuit that is operable to read the first authentication code from the first memory region, present the first authentication code to the comparator, and in response to receiving an indicator from the comparator indicating that the first and second authentication codes match, unlock at least one of (i) a communication interface of the chip to allow data to be transmitted therethrough to a chip reader and (ii) a third memory region of the chip to allow data to be read therefrom.

WO 2015/154185 A1

Published:

— *with international search report (Art. 21(3))*

SELF-AUTHENTICATING CHIPS

CROSS-REFERENCE TO RELATED APPLICATION

[0001] The present application claims priority to U.S. Patent Application No. 14/249244 filed April 9, 2014, titled "Self-Authenticating Chips", the contents of which is incorporated herein by reference.

TECHNICAL FIELD

[0002] This relates to microchips, and more particularly to self-authenticating microchips for inclusion in devices to protect against counterfeiting of such devices.

BACKGROUND

[0003] Each year, billions of dollars are lost worldwide to payment card fraud. Commonly, card data (*e.g.*, credit/debit card account number, expiry date, etc.) are copied by fraudsters to create counterfeit cards that are used to conduct fraudulent transactions. For example, card data stored on a card's magnetic stripe may be copied when an unwitting user swipes the card in a compromised merchant point-of-sale (POS) terminal. Further, the proliferation of Internet use and e-commerce has created new opportunities for card data to fall into unscrupulous hands.

[0004] Some technological advances have been made in recent years to combat counterfeiting of payment cards. For example, card issuers have introduced so-called "smart cards" that rely on embedded integrated circuits or microchips (hereinafter referred to as "smart chips" or "chips") to provide certain security features. For example, smart cards may be configured to require user authentication (*e.g.*, by entry of a secret numerical code) at the time of each transaction. Further, smart cards may be configured to communicate card data to merchant POS terminals in encrypted form to prevent that data from being copied. However, sophisticated fraudsters have discovered ways to replicate smart cards while circumventing the requirement for user authentication.

[0005] In recent years, counterfeiting of subscriber identity module (SIM) cards for mobile telephony devices has also emerged as a serious problem. Counterfeit SIM cards have been used by fraudsters to gain fraudulent access to mobile networks, and have also been used by criminals to commit crimes under fake or assumed identities. Conventional SIM cards include a number of security features to prevent counterfeiting. For example, conventional SIM cards include integrated circuits (chips) that store a secret key used to authenticate the SIM card to a mobile network. However, as is the case with smart cards, sophisticated fraudsters have discovered ways to replicate conventional SIM cards while circumventing their security features.

[0006] Accordingly, there is a need for improved protection against counterfeiting.

SUMMARY

[0007] According to an aspect, there is provided a self-authenticating chip. The chip includes a first memory region storing a first authentication code; a second memory region storing a second authentication code, the second memory region adapted to be unreadable and unmodifiable by the chip or a chip reader; a comparator interconnected to the second memory region for providing an indicator of whether given input matches the second authentication code; and an authentication circuit interconnected to the comparator and the first memory region. The authentication circuit is operable to: read the first authentication code from the first memory region; present the first authentication code to the comparator; and in response to receiving an indicator from the comparator indicating that the first authentication code matches the second authentication code: unlock at least one of (i) a communication interface of the chip to allow data to be transmitted therethrough to a chip reader and (ii) a third memory region of the chip to allow data to be read therefrom.

[0008] According to other aspects there is provided a card, a document, an electronic device, and a vehicle, each including a self-authenticating chip as disclosed herein.

[0009] According to another aspect, there is provided a self-authenticating card comprising: a first chip having a first memory region storing a first authentication code, and a communication interface for communicating with a chip reader; and a second chip having a second memory region storing a second authentication code. At least one of the first and second chips provides an authentication circuit interconnected with the first memory region and the second memory region, the authentication circuit operable to: read the first authentication code from the first memory region; read the second authentication code from the second memory region; authenticate the card by comparing the first authentication code with the second authentication code; and upon the authenticating: unlock at least one of (i) the communication interface to allow data to be transmitted therethrough (ii) a third memory region to allow data to be read therefrom.

[0010] According to a further aspect, there is provided an authentication system comprising: a self-authenticating chip as described herein or a self-authenticating card as described herein, and a computing device. The computing device includes a radio-frequency receiver, a network communication interface, at least one processor, and memory interconnected to the at least one processor. The memory stores software code that, upon execution by the at least one processor, causes the computing device to: receive a network authentication code from the self-authenticating chip or the first chip of the self-authenticating card, by way of the radio-frequency receiver; and transmit the network authentication code to a network-interconnected authentication server by way of the network communication interface.

[0011] Other features will become apparent from the drawings in conjunction with the following description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] In the figures which illustrate example embodiments,

[0013] **FIG. 1** is a schematic diagram of a device including a self-authenticating chip, exemplary of an embodiment;

[0014] **FIG. 2** is a network diagram illustrating a data communication network interconnecting a merchant POS terminal and a remote server, and a payment card including the self-authenticating chip of **FIG. 1**;

[0015] **FIG. 3A** and **FIG. 3B** are front and rear views, respectively, of the card of **FIG. 2**;

[0016] **FIG. 3C** is a schematic diagram of components of the card of **FIG. 2**;

[0017] **FIG. 4** is a simplified block diagram of the chip of **FIG. 1**;

[0018] **FIGS. 5A-C** are flowcharts depicting exemplary blocks performed by the chip of **FIG. 1**;

[0019] **FIG. 6** is a schematic diagram of components of a card including a self-authenticating chip, exemplary of another embodiment;

[0020] **FIG. 7** is a simplified block diagram of the chip of **FIG. 6**;

[0021] **FIG. 8** is a schematic diagram of components of a card including a self-authenticating chip, exemplary of yet another embodiment;

[0022] **FIG. 9** is a simplified block diagram of the chip of **FIG. 8**;

[0023] **FIG.10** is a network diagram illustrating a data communication network interconnecting a computing device and a remote server, and the payment card of **FIG. 2**, exemplary of another embodiment;

[0024] **FIG. 11** is a high-level block diagram of the computing device of **FIG. 10**;

[0025] **FIG. 12** is a flowchart depicting exemplary blocks performed by the computing device of **FIG. 10**;

[0026] **FIG. 13** is a network diagram illustrating a data communication network interconnecting a merchant POS terminal and a remote server, and a mobile phone including a self-authenticating chip, exemplary of another embodiment; and

[0027] **FIG. 14** is a front view of a passport document including a self-authenticating chip, exemplary of another embodiment.

DETAILED DESCRIPTION

[0028] **FIG. 1** depicts a self-authenticating chip **10** exemplary of an embodiment. As will become apparent, chip **10** performs authentication operations to verify its authenticity. As will also become apparent, when chip **10** is included in a device such as device **12**, chip **10** may be used to verify the authenticity of the device, and thereby protect against counterfeiting of the device. For example, chip **10** may be included in a payment card to verify the authenticity of the payment card when used to conduct a transaction. Self-authenticating chips as discussed herein may also be included in other types of devices such as, for example, SIM cards, identity cards or documents, electronic appliances, and vehicles, as further discussed below.

[0029] **FIG. 2** depicts a device **12** that is a payment card (hereinafter referred to as card **12**). As depicted, card **12** is presented to a merchant POS terminal **14** to conduct a transaction (*e.g.*, a credit card or debit card transaction). Presenting card **12** to terminal **14** causes chip **10** of card **12** to perform authentication operations, as detailed below. The transaction is allowed to proceed only if the authenticity of card **12** is verified upon performing these authentication operations.

[0030] An example merchant POS terminal **14** is illustrated. Terminal **14** may be a conventional device, as produced by, *e.g.*, VeriFone, Hypercom, or Ingenico, and is operated in manners detailed below. Terminal **14** is typically located at a merchant's premises and is used to conduct payment card transactions (*e.g.*, credit card or debit card transactions) between a merchant and a card bearer. As detailed below, when a transaction is conducted, terminal **14** obtains card data from a card (*e.g.*, card **12**) and transmits this data to a remote server **16**. To this end, terminal **14** is configured to communicate with card **12**, as well as network-interconnected server **16**.

[0031] In the depicted embodiment, terminal **14** includes an LCD display for displaying information to a user, a keypad for receiving user input, a slot through which

the magnetic stripe of a card (*e.g.*, card **12**) can be swiped to allow terminal **14** to read from that stripe, a slot for receiving a card with a smart chip to allow terminal **14** to communicate with that smart chip by way of the chip's contact pins, a radio-frequency (RF) interface to allow terminal **14** to communicate with the smart chip by way of RF signals, and a network interface to allow terminal **14** to communicate with a remote server by way a data network.

[0032] An example server **16** is illustrated. Server **16** may be a conventional server-class computing device adapted to service requests to process payment card transactions (*e.g.*, credit card or debit card transactions). Server **16** is typically operated by the issuer of the payment card or a delegate of the issuer.

[0033] The architecture of server **16** is not specifically illustrated. Server **16** may include one or more processors, memory, and a network interface to allow server **16** to communicate with network-interconnected merchant POS terminals (*e.g.*, terminal **14**). Server **16** may store and execute a network-aware server operating system (*e.g.*, Unix, Linux, Windows Server, or the like). Server **16** may be in communication with one or more databases storing credit card data and card bearer data.

[0034] As illustrated, terminal **14** and server **16** are interconnected by data network **18**. Data network **18** may include any combination of wired and wireless links capable of carrying packet-switched traffic. For example, these links may include links of a cellular data network (*e.g.*, a GPRS or LTE network) and/or the public Internet.

[0035] **FIG. 3A** and **FIG. 3B** respectively depict the front and rear of card **12**. As depicted, the exterior of card **12** is similar to a conventional smart card. In particular, card **12** has plastic front and rear surfaces, with contact pins **20** of chip **10** exposed on its front surface and magnetic stripe **24** affixed to its rear surface. In some embodiments, the front surface of card **12** may also include additional features such as, *e.g.*, the card bearer's name, the card's account number, and the card's expiry date, printed or embossed thereon. Similarly, in some embodiments, the rear surface of card **12** may also include additional features such as, *e.g.*, a security code or a signature panel.

[0036] In the depicted embodiment, card **12** is dimensioned to be readily carried by a user (*e.g.*, in a wallet). For example, card **12** may have dimensions that accord with published international standards such as ISO/IEC 7810. In embodiments that conform to the ID-1 format defined by the ISO/IEC 7810 standard, card **12** has a width of approximately 85.60 mm, a height of approximately 53.98 mm, and a thickness of approximately 0.76 mm. The dimensions of card **12** (*e.g.*, thickness, width, and height) may vary in other embodiments. Card **12** may be formed to have other physical characteristics (*e.g.*, flammability, toxicity, stiffness, durability, etc.) that accord with the ISO/IEC 7810 standard.

[0037] As depicted in **FIG. 3B**, card **12** includes magnetic stripe **24** storing data readable by a magnetic-stripe reader. Magnetic stripe **24** may be a conventional magnetic stripe storing data readable by a conventional magnetic stripe reader (*e.g.*, of merchant POS terminal **14**). As such, magnetic stripe **24** may store data in a plurality of bits positions, where each bit position can be set to a value of 0 or 1 by altering the state of magnetic domains at that bit position. In some embodiments, magnetic stripe **24** may store data in a format that accords with published international standards such as ISO/IEC 7811. So, magnetic stripe **24** may be organized to store data in three separate data tracks, namely, track 1, track 2, and track 3. When it is unnecessary for card **12** to provide data to a magnetic stripe reader, magnetic stripe **24** may be omitted.

[0038] **FIG. 3C** schematically illustrates components of card **12**, exemplary of an embodiment. As shown, card **12** includes chip **10**, and optionally, may also include an embedded power supply **26** connected to chip **10**. Chip **10** may be a conventional smart chip, such as, for example, a Siemens SLE4442 chip. Chip **10** includes logic adapting it to perform authentication operations in manners detailed below. Power supply **26** supplies power to card **12**, allowing card **12** to be operated when it cannot draw power from an external source, *e.g.*, from a merchant POS terminal by way of contact pins **20**. In an embodiment, power supply **26** may include a thin, flexible lithium polymer battery, as manufactured by, for example, Solicore of Lakeland, Florida.

[0039] **FIG. 4** is a simplified block diagram of chip **10**, exemplary of an embodiment. As depicted, chip **10** includes an authentication circuit **36** that includes logic for performing authentication operations. In particular, authentication circuit **36** includes logic for performing authentication by chip **10** itself, hereinafter referred to as "self-authentication". In some embodiments, authentication circuit **36** may also include logic for performing authentication in cooperation with a network-interconnected server (*e.g.*, server **16**), hereinafter referred to as "network authentication." The logic of authentication circuit **36** may be implemented using a combination of hardware and software components, including, *e.g.*, software code stored in EEPROM.

[0040] Chip **10** also includes memory regions **30** and **32**, which each store data, *i.e.*, authentication codes, used to perform the aforementioned self-authentication. Memory region **30** is interconnected with authentication circuit **36** such that data stored in memory region **30** may be read therefrom by authentication circuit **36**. Memory region **30** may be a region in any memory of chip **10** that may be read by authentication circuit **36**, *e.g.*, EEPROM or ROM. In other embodiments, memory region **30** may be a region in a memory external to chip **10**.

[0041] Memory region **32** is a protected memory region that is adapted to be unreadable and unmodifiable by chip **10** or a chip reader. Memory region **32** is interconnected with comparator **34** such that data stored in memory region **32** is presented to input A of comparator **34**. Data written to memory region **32** can only be accessed by presenting data to input B of comparator **34**, which outputs a binary indicator of whether data at input A matches data at input B. In embodiments in which chip **10** is a Siemens SLE4442 chip, memory region **32** may be located in the Manufacturer's Code partition of this Siemens chip.

[0042] As depicted, chip **10** also includes an I/O interface **38** that allows chip **10** to communicate with a chip reader such as a merchant POS terminal, a computing device as described below, or other devices adapted to communicate with a conventional smart card (collectively, "chip readers" or "card readers"). In particular, interface **38** allows chip **10** to communicate with a chip reader by way of contact pins

20. Optionally, interface **38** may also allow chip **10** to communicate with a chip reader by way of RF signals. To facilitate RF communication, interface **38** may include an RF transmitter and an RF receiver, interconnected with an RF antenna embedded in card **12** (not shown). In some embodiments, such RF communication may adhere to the near field communication (NFC) protocol.

[0043] Interface **38** may be selectively lockable to prevent data from being communicated therethrough from chip **10** to a chip reader (*e.g.*, terminal **14**). For example, when chip **10** is included in payment card **12**, locking interface **38** may prevent payment card account data to be transmitted to a chip reader before chip **10** has verified its authenticity. Interface **38** may be locked, for example, by disabling a RF transmitter of chip **10** and/or disabling one or more pins of contact pins **20**. Interface **38** may be toggled between locked and unlocked states in response to a signal, *e.g.*, sent by authentication circuit **36**.

[0044] Optionally, chip **10** may also include a memory region **40** that stores data to be provided to a chip reader after chip **10** performs self-authentication. As depicted, memory region **40** is interconnected with authentication circuit **36**. In some embodiments, memory region **40** may be formed in selectively lockable memory as disclosed, for example, in U.S. Patent No. 8,051,263 to Renno. Memory region **40** may be toggled between locked and unlocked states in response to a signal, *e.g.*, sent by authentication circuit **36**. When memory region **40** is locked, access to data stored therein is disabled. For example, when chip **10** is included in payment card **12** and payment card account data is stored in memory region **40**, locking memory region **40** prevents that data from being read from memory region **40** and transmitted from chip **10** before chip **10** has verified its authenticity.

[0045] When chip **10** is included in a device that is a payment card (*e.g.*, card **12**), chip **10** may also include other components of a conventional payment card smart chip, which are not shown in **FIG. 4** or detailed herein.

[0046] **FIG. 5A** and **FIG. 5B** depict exemplary operations performed by chip **10** during self-authentication. As will be detailed below with reference to blocks **S500** and

onward, chip **10** performs self-authentication by comparing a first chip authentication code stored at a first location on chip **10** with a second chip authentication code stored at a second location on chip **10**. Chip **10** is verified to be authentic only if these two codes match. In some embodiments, the first and second chip authentication codes may be identical. In other embodiments, these codes may be related by a defined relationship (*e.g.*, a hash function), allowing the codes to be matched according to the defined relationship.

[0047] The chip authentication codes may be assigned to chip **10** at time of manufacture, and may be unique to chip **10**. When chip **10** is included in a device (*e.g.*, card **12**), that device may be deemed to be authentic when chip **10** is verified to be authentic.

[0048] Chip **10** is initialized prior to performing self-authentication. In particular, a first chip authentication code is written to a first location (*e.g.*, protected memory region **32**), and a second chip authentication code is written to a second location (*e.g.*, memory region **30**).

[0049] As noted, when a chip authentication code is written to protected memory region **32**, it cannot be read or modified by chip **10** or any external reader/writer. Rather, comparator **34** must be used to compare given input to the code in protected memory region **32**.

[0050] In some embodiments, the second chip authentication code may be stored in encrypted form. Conventional encryption techniques may be used for this purpose. For example, a symmetric-key encryption technique such as, *e.g.*, AES, DES, 3DES, or the like may be used. Alternatively, an asymmetric-key encryption technique such as RSA may also be used. Other encryption techniques apparent to a person skilled in the art may also be used instead of or in conjunction with the techniques listed above. In some embodiments, customized or proprietary encryption techniques may also be used. The key(s) may be unique to chip **10**.

[0051] Conveniently, when the first chip authentication code is stored in protected memory region **32** and the second chip authentication code is stored in encrypted form, the chip authentication codes cannot be read from chip **10** by a would-be fraudster, *e.g.*, using a compromised merchant POS terminal. This prevents duplication of the chip authentication codes of chip **10**. When chip **10** is included a device (*e.g.*, card **12**), this protects against counterfeiting of that device.

[0052] Furthermore, as two chip authentication codes are required to perform self-authentication, any counterfeit device that replicates only one of these codes would not be able to successfully perform self-authentication. For example, a counterfeit copy of card **12** that replicates the first chip authentication code without replicating the second chip authentication code in protected memory region **32** would not be able to successfully perform self-authentication.

[0053] During initialization, authentication circuit **36** may send lock signals to one or both of authentication circuit **36** and memory **40**.

[0054] With reference to **FIG. 5A**, chip **10** begins performing blocks **S500** and onward when a chip reader initiates communication with chip **10**, *e.g.*, when a merchant POS terminal such as terminal **14** initiates communication with chip **10** to conduct a transaction. In some embodiments, chip **10** may perform blocks **S500** and onward upon receiving a signal indicating a user request to perform self-authentication.

[0055] At block **S502**, authentication circuit **36** reads the first chip authentication code from memory region **30**. If the code is encrypted, authentication circuit **36** decrypts it. At block **S504**, authentication circuit **36** presents the first chip authentication code to input B of comparator **34**. At the same time, the second chip authentication code stored in protected memory region **32** is presented to input A of comparator **34**.

[0056] At block **S506**, comparator **34** determines whether the first chip authentication code presented at its input A matches the second chip authentication

code presented at its input B. Comparator **34** outputs an indicator indicating whether the two codes match to authentication circuit **36**. If this indicator indicates a match, then operation of chip **10** is allowed to continue. Otherwise, operation of chip **10** may be terminated. For example, when chip **10** is included in payment card **12**, and self-authentication is performed prior to completing a transaction, operation of chip **10** may be terminated such that chip **10** cannot be used to complete that transaction.

[0057] As noted, interface **38** may be locked until chip **10** has verified its authenticity by performing self-authentication. Accordingly, at block **S508**, after chip **10** has verified its authenticity, authentication circuit **36** may transmit an unlock signal to interface **38** thereby unlocking interface **38** and allowing data to be transmitted therethrough.

[0058] In another embodiment, instead of or in addition to unlocking interface **38**, authentication circuit **36** may also send an unlock signal to memory region **40**, thereby unlocking memory region **40** and allowing data to be read therefrom.

[0059] At block **S510** (**FIG. 5B**), authentication circuit **36** reads chip data from memory of chip **10** (*e.g.*, from memory region **40**), and at block **S512**, authentication circuit **36** transmits this chip data to a chip reader (*e.g.*, terminal **14**) by way of interface **38**. When chip **10** is included in payment card **12**, this chip data may be payment card account data for conducting a payment card transaction.

[0060] Once this chip data has been transmitted to the chip reader, operations at chip **10** may cease until self-authentication needs to be performed once again. If interface **38** was unlocked at block **S508**, then it may again be locked by sending a lock signal from authentication circuit **36**. Similarly, if memory region **40** was unlocked at block **S508**, then it may again be locked by sending a lock signal from authentication circuit **36**.

[0061] As noted, in some embodiments, authentication circuit **36** may also include logic for performing network authentication in cooperation with a remote server such as server **16**. In particular, network authentication is performed by comparing a network authentication code stored at chip **10** with a network authentication code

stored at server **16**, and chip **10** is verified to be authentic only if the codes match. The network authentication codes stored respectively at chip **10** and at server **16** may be identical or matched according to a defined relationship (*e.g.*, a hash function).

[0062] The network authentication codes stored at chip **10** and server **16** may be changed from time to time. Conveniently, updating the network authentication codes from time to time ensures that, in the event that a network authentication code is copied to a counterfeit card, that network authentication code may only be used to successfully complete network authentication for a limited time, *e.g.*, until the network authentication code changes.

[0063] The network authentication codes stored at chip **10** and server **16** may be updated synchronously. For example, in some embodiments, the codes may be updated at predetermined time intervals (*e.g.*, every 30 minutes). These codes are changed in such a way that they remain matching after each change. For example, the network authentication codes may be changed at chip **10** and at server **16** according to a predetermined sequence, which may be a pseudo-random sequence, or according to a predetermined code-generation algorithm.

[0064] The network authentication codes may include, or be generated from, a current timestamp (*e.g.*, indicating time and date). A device having a chip with a stale timestamp or sequence value may be readily identified as being a counterfeit.

[0065] The network authentication codes may be updated at chip **10** and server **16** each time card **12** is used in a transaction. So, the network authentication codes may include, or be generated using a transaction identifier that uniquely identifies each transaction. Of course, the network authentication codes may include, or be generated from both a network identifier and a timestamp.

[0066] Optionally, when network authentication is performed, the network authentication code at chip **10** may be allowed to deviate by a predefined margin from the network authentication code at server **16**. For example, if the network authentication codes include timestamps, then the respective timestamps of the two

network authentication codes may be allowed to deviate by a predefined time interval (*e.g.*, 30 seconds, one minute, etc.). Similarly, if the network authentication codes include transaction identifiers, then the respective transaction identifiers of the two network authentication codes may be allowed to deviate by a predefined number of transactions. In this way, network authentication may be allowed to complete successfully even if the network authentication codes do not match exactly.

[0067] The operation of an embodiment of chip **10** that performs network authentication is further described with reference to the exemplary blocks shown in **FIG. 5A** and **FIG. 5C**. In this embodiment, the above initialization steps further include initializing chip **10** to perform network authentication before blocks **S500** and onward are performed. In particular, chip **10** is initialized by writing an initial network authentication code to memory of chip **10**.

[0068] This network authentication code may be written to memory region **40** of chip **10**. In this case, the network authentication code may not be accessible until memory region **40** is unlocked following successful self-authentication. However, the network authentication code may also be written to another memory region in chip **10** (*e.g.*, memory region **30**) or memory that is external to chip **10** but accessible by chip **10**.

[0069] The network authentication code stored in memory of chip **10** or accessible by chip **10** may be stored in encrypted form using any of the encryption techniques described above. In an embodiment, the chip authentication code described above may be used as the symmetric key for encrypting/decrypting the network authentication code at chip **10**. Conveniently, this ensures that the network authentication code can only be decrypted using the chip authentication code, which as noted above, cannot be copied by would-be fraudsters.

[0070] In this embodiment of **FIG. 5A** and **FIG. 5C**, self-authentication is performed, as depicted in **FIG. 5A** and detailed above. However, following successful self-authentication, network authentication operations are performed. In particular, at block **S514**, authentication circuit **36** reads the network authentication code from memory in

chip **10** (*e.g.*, memory region **40**). Next, this network authentication code is sent by authentication circuit **36** to interface **38**, which transmits the code to terminal **14**.

[0071] Terminal **14** then relays the network authentication code of chip **10** to server **16**, where it is compared against the network authentication code stored at server **16**. Server **16** determines chip **10** to be authentic if the network authentication code of chip **10** matches the network authentication code of server **16**. When chip **10** is included in card **12**, if chip **10** is determined to be authentic, then card **12** is deemed to be authentic.

[0072] Along with the network authentication code, chip **10** may also transmit other data stored at the chip to terminal **14**, for relay to server **16**. For example, this other data may be a payment card account number required to conduct a transaction.

[0073] The network authentication code and other data stored at chip **10** may be transmitted to terminal **14** in encrypted form for relay to server **16**. In this way, this code and data are protected from being copied at terminal **14** or during subsequent transmission to server **16**. Chip **10** may additionally send a unique chip identifier to server **16** in unencrypted form to allow server **16** to select the appropriate decryption key.

[0074] After network authentication has been performed, chip **10** may update its network authentication code. In particular, at block **S518**, authentication circuit **36** generates a new network authentication code in manners described above, and at block **S520**, stores the new network authentication code, *e.g.*, in memory **40**. As noted above, the network authentication code may be stored in encrypted form. At this time, a new network authentication code is also generated and stored at server **16**, to be used during a subsequent network authentication process.

[0075] When smart chip **10** updates its network authentication code while connected to an external power source (*e.g.*, terminal **14** by way of contact pins **22**), chip **10** may draw power from that external power source. When chip **10** updates the network

authentication code at other times, it may draw power from an embedded power supply such as power supply **26** (**FIG. 3C**).

[0076] Optionally, following self-authentication, chip **10** may also perform a user authentication process. For example, the user may be prompted to enter a numeric code (*i.e.*, secret PIN) by way of the keypad of terminal **14**, which is then verified by smart chip **10**.

[0077] **FIG. 6** schematically illustrates the internal components of a card **12'**, exemplary of another embodiment. Card **12'** is substantially similar to card **12**, but includes a chip **10'** instead of a chip **10**. Card **12'** further includes a second chip **11** interconnected with chip **10'** by way of data connection **44**, allowing data to be transmitted therebetween. Like card **12**, card **12'** may optionally include an embedded power supply **26**.

[0078] Connection **44** may be formed using suitable nanotechnologies, *e.g.*, using conductive carbon nanowires. Conveniently, as will be appreciated, carbon nanowires may be smaller and/or lighter than conventional conductors. Further, carbon nanowires may exhibit improved durability, improved thermal stability, and higher magnetic coercivity compared to conventional conductors.

[0079] Chip **10'** is substantially similar to chip **10**, aside from the differences described herein. In particular, as detailed below, chip **10'** cooperates with chip **11** to perform self-authentication. Chip **10'** may also cooperate with chip **11** to perform network authentication in conjunction with a network-interconnected server such as server **16**.

[0080] Chip **11** may be a conventional smart chip, such as, for example, a Siemens SLE4442 chip, and includes logic adapting it to operate in manners detailed below. Unlike chip **10'**, which has contact pins exposed to the exterior of card **12'**, chip **11** may be substantially sealed within card **12'**. Conveniently, this protects chip **11** from physical contact with a chip reader and may improve security against possible tampering or unauthorized access to data stored in chip **11**. Chip **11** may be adapted

to communicate only with chip **10**, in response to communication initiated by chip **10**. Thus, chip **11** may ignore communication originating from other sources, *e.g.*, a merchant POS terminal.

[0081] **FIG. 7** is a simplified block diagram of chip **10'**, exemplary of an embodiment. As depicted, chip **10'**, like chip **10**, also includes a protected memory region **32** storing a chip authentication code, a comparator **34** allowing given input to be compared to the chip authentication code stored in protected memory region **32**, an authentication circuit **36** that includes logic for performing authentication operations, an I/O interface **38** that allows chip **10'** to communicate with a chip reader, and optionally, a memory region **40** that stores data to be provided to a chip reader.

[0082] Unlike chip **10**, chip **10'** does not include a memory region **30** interconnected with authentication circuit **36** that stores a second chip authentication code for comparison with the first chip authentication code stored in protected memory region **32**. The second chip authentication code is instead stored in a memory of chip **11**, and this memory of chip **11** is interconnected with authentication circuit **36** such that the second chip authentication code may be read therefrom by authentication circuit **36**.

[0083] Authentication circuit **36** presents the second chip authentication code read from chip **11** to input B of comparator **34**. Comparator **34** compares the second chip authentication code to the first chip authentication code stored in memory region **32** and presented at input A of comparator **34**. Comparator **34** outputs a binary indicator of whether these two chip authentication codes match. Thus, chips **10'** and **11** cooperate to perform the blocks shown in **FIG. 5A** and **FIG. 5B** to verify that that the chips are authentic, and that card **12'** is authentic.

[0084] Optionally, chip **10'** may also perform network authentication as shown in **FIG. 5C** in substantially the same manner as described above. However, the network authentication code to be sent to server **16** may be read from a memory of chip **11**, and may be updated by authentication circuit **36** by writing a new network authentication code to memory of chip **11**.

[0085] In another embodiment, one or more of memory region **32**, comparator **34**, and authentication circuit **36** may be moved from chip **10'** to chip **11**. Since chip **11** is substantially sealed within card **12'**, moving components from chip **10'** to chip **11** may improve security against possible tampering or unauthorized access.

[0086] **FIG. 8** schematically illustrates the internal components of a card **12''**, exemplary of yet another embodiment. Card **12''** is substantially similar to card **12**, but includes a chip **10''** instead of a chip **10**. Card **12''** further includes components allowing chip **10''** to read and write to magnetic stripe **24**. In particular, card **12''** further includes a write circuit **46** interconnected to chip **10''** by way of data connection **52**, allowing chip **10''** to write data to at least part of magnetic stripe **24**, and a read circuit **48** interconnected to chip **10''** by way of a data connection **50**, allowing chip **10''** to read from at least part of magnetic stripe **24**. Card **12''** may also include a swipe detector **36** that detects when the card has been swiped through a magnetic stripe reader (*e.g.*, of merchant POS terminal **14**). Like card **12**, card **12''** may optionally include an embedded power supply **26**.

[0087] Write circuit **46** includes at least one write head that operates under control of chip **10''** to set the magnetic state of particular bit positions of magnetic stripe **24**. Each write head may include a magnetic transducer that converts a signal from chip **10''** to magnetic energy to set the state of magnetic domains at one or more bit positions of magnetic stripe **24**, thereby storing a value of 0 or 1 at each of those bit positions. In an embodiment, multiple write heads may be arranged in an array along the magnetic stripe **24** to write to respective bit positions along the stripe. In some embodiments, write circuit **46** may include write heads as described in U.S. Patent No. 7,044,394 to Brown. In other embodiments, write circuit **46** may include write heads formed as an array or a multi-dimensional matrix of conductors, as described in, *e.g.*, International Patent Publication WO 2004/095169 to Osterweil or U.S. Patent No. 7,591,427 to Osterweil. The array/matrix of conductors may be embedded in card **12''** proximate magnetic stripe **24**.

[0088] Data written to magnetic stripe **24** may be read by chip **10''** by way of read circuit **48**, as detailed below, or by a magnetic stripe reader (*e.g.*, of merchant POS terminal **14**) upon swiping card **12''** through the reader.

[0089] Read circuit **48** includes at least one read head that operates under control of chip **10''** to read the magnetic state of particular bit positions of magnetic stripe **24**. Each read head may include a sensor that senses the state of magnetic domains at one or more bit positions of magnetic stripe **24** and generates a signal representative of that state (*e.g.*, indicating a value of 0 or 1 for a particular bit position). In an embodiment, multiple read heads may be arranged in an array along magnetic stripe **24** to read from respective bit positions along the stripe. In some embodiments, read circuit **48** may include read heads that sense the magnetic state of particular bit positions using fluxgate sensors, *e.g.*, as described in U.S. Patent No. 7,591,427 to Osterweil.

[0090] In some embodiments, a single circuit may be used for both reading and writing. For example, this circuit may include write-heads adapted to also read from a magnetic stripe, or read-heads adapted to also write to a magnetic stripe.

[0091] Given the relative thinness of card **12''** in some embodiments, one or both of write circuit **46**, read circuit **48**, and data connections **50** and **52** may be formed using suitable nanotechnologies, *e.g.*, using conductive carbon nanowires.

[0092] Swipe detector **54** detects when card **12''** has been swiped through a magnetic stripe reader (*e.g.*, of terminal **14**). In some embodiments, swipe detector **54** includes a pressure sensor to detect pressure applied to card **12''** when it is swiped through a merchant POS terminal. In other embodiments, swipe detector **54** includes a sensor that detects the electromagnetic signature of magnetic stripe reader, *e.g.*, of the reader's read heads. In some embodiments, swipe detector **54** includes read-head detectors as described in U.S. Patent Publication 2012/0318871 to Mullen *et al.*

[0093] **FIG. 9** is a simplified block diagram of chip **10''**, exemplary of an embodiment. As depicted, chip **10''**, like chip **10**, also includes a protected memory

region **32** storing a chip authentication code, a comparator **34** allowing given input to be compared to the chip authentication code stored in protected memory region **32**, an authentication circuit **36** that includes logic to control chip **10''** to perform authentication operations, an I/O interface **38** that allows chip **10''** to communicate with a chip reader, and optionally, a memory region **40** that stores data to be provided to a chip reader.

[0094] Unlike chip **10**, chip **10''** does not include a memory region **30** interconnected with authentication circuit **36** that stores a second chip authentication code for comparison with the first chip authentication code stored in protected memory region **32**. The second chip authentication code is instead stored on magnetic stripe **24**, and is read therefrom by authentication circuit **36** by way of read circuit **48**.

[0095] Authentication circuit **36** presents the second chip authentication code read from the magnetic stripe **24** to input B of comparator **34**. Comparator **34** compares this second chip authentication code to the first chip authentication code stored in memory region **32** and presented at input A of comparator **34**. Comparator **34** outputs a binary indicator of whether these two chip authentication codes match. Thus, chip **10''** performs the blocks shown in **FIG. 5A** and **FIG. 5B** to verify that that the chip is authentic, and that card **12'** is authentic.

[0096] Optionally, chip **10'** may also perform network authentication as shown in **FIG. 5C** in substantially the same manner as described above. However, the network authentication code to be sent to server **16** may be read from magnetic stripe **24** by way of read circuit **48**, and may be updated by authentication circuit **36** by writing a new network authentication code to magnetic stripe **24** by way of write circuit **46**.

[0097] Conveniently, storing a network authentication code on magnetic stripe **24** provides for compatibility with merchant POS terminals that are unable to communicate with chip **10''** but are able to read from magnetic stripe **24**. In particular, the network authentication code may be read by the merchant POS terminal when card **12''** is swiped through the terminal, and the code may then be passed to server **16** to perform network authentication.

[0098] When card **12''** is used to conduct a transaction in conjunction with a merchant POS terminal that reads from magnetic stripe **24** without communicating with chip **10''**, chip **10''** relies on a signal from swipe detector **54** indicating that card **12''** has been swiped through a merchant POS terminal. In response, chip **10''** may update the network authentication code in manners described above, *e.g.*, by generating a new network authentication code and writing this new code to magnetic stripe **24** by way of write circuit **46**.

[0099] In contrast to a conventional payment card that stores card data (*e.g.*, a credit/debit card account number, expiry date, etc.) on track 1 and track 2 of its magnetic stripe while leaving track 3 unused, in the embodiment depicted in **FIG. 8**, the chip authentication code and the network authentication code on magnetic stripe **24** are stored on track 3. In some embodiments, track 1 and track 2 of magnetic stripe **24** may continue to store card data in a conventional way. In other embodiments, track 1 and track 2 of magnetic stripe **24** may simply be left unused (blank), and card data may be stored on track 3 of magnetic stripe **24** instead. Any card data stored on track 3 of magnetic stripe **24** may be in encrypted form. Conveniently, conventional merchant POS terminals may be adapted to read from track 3 by updating its software/firmware, while avoiding any hardware changes.

[00100] As the first and second chip authentication code are stored at two separate locations on card **12'**, any counterfeit copy of card **12'** that replicates the data of only one of these locations would not be able to successfully perform self-authentication. For example, a counterfeit copy of card **12'** that only replicates the contents of magnetic stripe **24** would not be able to successfully perform self-authentication.

[00101] **FIG. 10** depicts payment card **12** including self-authenticating chip **10**, presented to a computing device **100** to conduct an e-commerce transaction with a merchant, exemplary of an embodiment. In this embodiment, the above-discussed self-authentication and network authentication operations are both performed. Conveniently, network authentication may be performed and the transaction may be

conducted in the absence of a merchant POS terminal, *e.g.*, when card **12** is used in the card bearer's home.

[00102] An exemplary computing device **100** is shown. Computing device **100** may be a device such as a desktop personal computer, a laptop computing device, a network computing device, a tablet computer, a personal digital assistant, a mobile phone, a smart television device, a video gaming console device, or the like, adapted to operate in the manner discussed below.

[00103] As shown in the high-level block diagram of **FIG. 11**, computing device **100** includes at least one processor **102** and memory **106** in communication with processor **102**. Memory **106** stores software code, that when executed by processor **102**, causes computing device **100** to conduct a payment card transaction (*e.g.*, a credit/debit card transaction) in cooperation with card **12** and server **16**.

[00104] As depicted, computing device **100** also includes RF interface **104** that allows device **100** to communicate with chip **10** of card **12** by way of RF communication. In some embodiments, RF interface **104** includes a peripheral communication port (*e.g.*, Universal Serial Bus, IEEE 1394, serial, parallel, or the like) that allows an RF transmitter and an RF receiver to be removably attached to computing device **100**. In other embodiments, RF interface **104** may include an integral RF transmitter and RF receiver, *e.g.*, where computing device **100** is a mobile phone or a tablet computer. In some embodiments, computing device **100** may communicate with chip **10** by way of RF interface **104** using the NFC protocol.

[00105] As depicted, computing device **100** also includes a network interface that allows device **100** to communicate with network-connected devices (*e.g.*, server **16**) by way of data network **18**. Computing devices **100** typically store and execute network-aware operating systems including protocol stacks, such as a TCP/IP stack. Computing device **100** may also store and execute web browsers such as Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari, or the like, to allow the bearer of card **12** to conduct web-based payment card transactions.

[00106] The operation of computing device **100** is further described with reference to **FIG. 12**, which depicts exemplary blocks performed by computing device **100** to conduct a payment card transaction. A transaction is initiated by a user (*e.g.*, the bearer of card **12**) operating computing device **100**, for example, with a remote merchant by way of a web site operated by that merchant. Computing device **100** then performs blocks **S1200** and onward.

[00107] At block **S1202**, computing device **100** transmits a signal by way of RF interface **104** to chip **10** indicating that a transaction has been initiated and requesting that chip **10** provide its network authentication code. Upon receiving this signal, chip **10** performs the authentication operations depicted in **FIG. 5A** and **FIG 5C**, as discussed above, including the self-authentication operation discussed above.

[00108] Chip **10** may refuse to provide the requested network authentication code if self-authentication fails, in which case the transaction is terminated. However, if self-authentication is performed successfully, at block **1204**, computing device **100** receives a network authentication code from chip **10** by way of RF interface **104**. At block **1206**, computing device **100** transmits the received network authentication code to server **16** by way of network interface **108**.

[00109] Computing device **100** may also transmit any additional card data (*e.g.*, a credit/debit card account number) received from chip **10** to server **16**. When data is received from chip **10** in encrypted form, computing device **100** may relay it to server **16** without decrypting that data.

[00110] Server **16** performs network authentication using the network authentication code relayed by computing device **100**, in manners described herein. Upon performing network authentication, server **16** may authorize or reject the transaction.

[00111] As will be appreciated, cards **12'** and **12"** may also be used to conduct transactions by way of computing device **100**, in substantially the same manner as card **12**.

[00112] A self-authenticating chip as disclosed herein may also be included in a SIM card. For example, **FIG. 13** depicts a SIM card **112** including a chip **110**. Chip **110** may be a conventional SIM chip that identifies a mobile service subscriber when used in a conventional mobile telephony device, but is adapted to also function in manners substantially similar to chip **10**. For example, in some embodiments, chip **110** may be a conventional SIM chip having at least 64 kilobytes of memory, capable of executing a conventional SIM Virtual Machine, and including or modified to include a protected memory region **32**.

[00113] As such, chip **110** performs self-authentication in manners described above for chip **10** to verify its authenticity. For example, chip **110** may verify its own authenticity before it provides subscriber identity data, such as an international mobile subscriber identity (IMSI) code to a mobile service provider server to gain access to mobile network resources. In particular, chip **110** may perform blocks **S500** and onward as depicted in **FIG. 5A** and **FIG. 5B**. Once chip **110** has verified its authenticity, subscriber identity data (*e.g.*, an IMSI code) is transmitted to a mobile telephony device for relay to a mobile service provider server at block **S512**.

[00114] Chip **110** may also verify its own authenticity each time particular mobile network resources are requested, *e.g.*, each time that a call is placed, or a Short Message Service (SMS) message is sent. Thus, a counterfeit SIM card may be prevented from accessing mobile network sources.

[00115] Optionally, chip **110** may also perform network authentication in manners described above for chip **10** and depicted in **FIG. 5C**, in cooperation with a mobile service provider server.

[00116] In some embodiments, chip **110** may be further adapted to include functionality of a conventional payment card smart chip. In particular, chip **110** may store in its memory payment card account data to conduct transactions, and may be adapted to communicate with an RF transmitter to conduct transactions with a merchant POS terminal, *e.g.*, using the NFC protocol. In such embodiments, chip **110** may be a conventional RF-enabled SIM chip, which may be modified to include a

protected memory region **32**, and adapted to function in manner substantially similar to chip **10**. Exemplary conventional RF-enabled RIM chips that could be used include, for example, SIM Model Nos. SGSIMRFA01, SGEMVSIM01, SGSIMNFC01, 15350F0, SGNFCSIM08, provided by Shenzhen Sunshine Good Electronic Company Limited (China); and Hengbao RF-SIM chips provided by Hengbao Co., Ltd. (Singapore).

[00117] Conveniently, adapting chip **110** to include functionality of a conventional payment card smart chip allows users to conduct payment transactions using a mobile telephony device including chip **110**, in lieu of a conventional payment card (*e.g.*, a credit card or a debit card).

[00118] Returning to **FIG. 13**, as depicted, chip **110** is included in SIM card **112** of mobile phone **120**. Mobile phone **120** is presented to merchant POS terminal **14** to conduct a transaction (*e.g.*, a credit card or debit card transaction) by way of RF communication. Presenting mobile phone **120** to terminal **14** causes chip **110** to perform authentication operations, namely, self-authentication, and optionally, network authentication as described above with reference to **FIGS. 5A-C**. Chip **110** transmits payment card account data stored in its memory to terminal **14** only upon successfully verifying its authenticity.

[00119] As will be appreciated, mobile phone **120** including chip **110** may also be used to conduct transactions by way of computing device **100** (**FIG. 10**), in substantially the same manner as card **12**.

[00120] In an embodiment, chip **110** in SIM card **112** may be adapted to transmit messages to a counterpart chip in the SIM card of another mobile telephony device. In this embodiment, chip **110** may verify its authenticity before sending such messages.

[00121] Optionally, chip **110** in SIM card **112** may store authentication codes for one or more counterpart chips in other SIM cards, *e.g.*, authentication codes for chips in other SIM cards used by contacts of the user of SIM card **112**. Such authentication codes may, for example, be serial numbers assigned to each of those SIM cards. Chip **110** may use the stored authentication codes to verify the authenticity of a counterpart

chip in another SIM card when a message is received from that chip. For example, when an incoming message is received by chip **110** from a given chip and the message includes an authentication code, chip **110** may compare the received authentication code with its stored authentication code for the given chip. If the codes match, then the given chip is verified to be authentic. Similarly, chip **110** may store its own authentication code, and may transmit this code to counterpart chips to allow those chips to verify the authenticity of chip **110**.

[00122] Chip **110** may also be adapted to perform self-authentication and/or network authentication in manners described above upon request from a software application executing at mobile phone **120**. For example, a mobile ticketing software application executing at mobile phone **120** may request that chip **110** verify its authenticity before providing an electronic ticket number to a ticket check station. A retailer's software application executing at mobile phone **120** may request that chip **110** verify its authenticity before providing a voucher code or a coupon code to a checkout station. A mobile money transfer software application executing at mobile phone **120** may request that chip **110** verify its authenticity before allowing a money transfer to be sent or received.

[00123] In some embodiments, software application data (*e.g.*, an electronic ticket number, a coupon code, a voucher code, or the like) may be provided to chip **110** and stored therein for later transmission to a chip reader. Of course, such data may be transmitted only after chip **110** verifies its authenticity.

[00124] SIM card **112** may be a GSM SIM card, a USIM card, a CSIM card, a R-UIM card, or a Universal Integrated Circuit Card, a high-capacity SIM card, a MegaSIM card, or the like.

[00125] In other embodiments, a self-authenticating chip as disclosed herein may be included in another type of card. For example, a self-authenticating chip may be included in an access card used to gain entry to a particular vehicle or a particular location (*e.g.*, a building, a room, a garage, etc.). A self-authenticating chip may also be included in a public transportation card for gaining access to a public transportation

service. A self-authenticating chip may also be included in an identity card, a membership card, a driver's license, a health care card, military personnel card, or the like. Conveniently, protecting against counterfeiting of such cards helps to prevent identity theft, unauthorized entry, and fraudulent access to services or funds.

[00126] In further embodiments, a self-authenticating chip as disclosed herein may be included in another type of device such as a document. For example, as depicted in **FIG. 14**, a self-authenticating chip **210** may be included in a passport **212**. Chip **210** may perform authentication operations as described above, and provide passport data (*e.g.*, the passport number, the passport holder's name) to a chip reader only upon verifying its authenticity. Similarly, a self-authenticating chip may be included in another type of document, such as a travel visa, a birth certificate, a diploma, or the like.

[00127] In yet further embodiments, a self-authenticating chip as disclosed herein may be included in network appliances such as a network router, a network switch, a modem, or the like, to perform authentication operations as described above before such gaining access to network resources. A self-authenticating chip as disclosed herein may also be included in television appliances such as a set-top box, a television, a Smart TV, or the like, to perform authentication operations as described above before gaining access to a television transmission.

[00128] In another embodiment, a self-authenticating chip as disclosed herein may be included in a motor vehicle to allow a payment transaction to be conducted in the absence of a payment card. When included in a motor vehicle, the chip may be used to pay for charges incurred in the course of operating the vehicle, *e.g.*, for drive-through restaurants, drive-in theatres, car washes, road tolls, parking, refueling, or the like. In particular, the chip may pay for such charges by transmitting stored payment data (*e.g.*, a payment card account number) to a POS terminal by way of RF communication. Of course, payment data may be transmitted from the chip only if it successfully verifies its authenticity upon performing self-authentication.

[00129] The self-authenticating chip may be interconnected to the power system of the vehicle to draw power therefrom. The chip may also be interconnected to a battery such as a long-lasting lithium battery or the like. Both the chip and the battery may be encased within a protective material such as epoxy or the like. To extend the range of RF communication, the chip may be connected to an antenna that extends along the vehicle body.

[00130] Conveniently, payments may be made automatically without manual intervention from either an occupant of the vehicle or a vendor. Of course, automatic payments may be governed by predefined rules, *e.g.*, to allow payments in amounts below a specified limit, payments to specified vendor types, or payments to specified vendors. Payment rules may be stored in memory of the self-authenticating chip.

[00131] Payment may also be manually requested by a user, *e.g.*, an occupant of the vehicle, by way of a user interface in communication with the self-authenticating chip. This user interface could be integral to the vehicle or mounted thereto. For example, it could be installed on the vehicle dashboard or steering wheel. The user interface could also be part of a separate computing device (*e.g.*, a mobile phone) operated by an occupant of the vehicle.

[00132] The chip may also store data other than payment data, such as data reflective of vehicle registration, Vehicle Identification Numbers (e.g., chassis and engine numbers), manufacturer's information, a driver's license, or insurance information. Such data may be transmitted by the chip by way of RF communication in response to an inquiry, *e.g.*, from a device operated by law enforcement, border control, or the like. The chip may perform self-authentication before transmitting such data.

[00133] Of course, the above described embodiments are intended to be illustrative only and in no way limiting. The described embodiments are susceptible to many modifications of form, arrangement of parts, details and order of operation. The invention is intended to encompass all such modification within its scope, as defined by the claims.

WHAT IS CLAIMED IS:

1. A self-authenticating chip comprising:

a first memory region storing a first authentication code;

a second memory region storing a second authentication code, said second memory region adapted to be unreadable and unmodifiable by said chip or a chip reader;

a comparator interconnected to said second memory region for providing an indicator of whether given input matches said second authentication code; and

an authentication circuit interconnected to said comparator and said first memory region;

said authentication circuit operable to:

read said first authentication code from said first memory region;

present said first authentication code to said comparator; and

in response to receiving an indicator from said comparator indicating that said first authentication code matches said second authentication code:

unlock at least one of (i) a communication interface of said chip to allow data to be transmitted therethrough to a chip reader and (ii) a third memory region of said chip to allow data to be read therefrom.

2. The chip of claim 1, wherein said communication interface comprises a radio-frequency transmitter.

3. The chip of claim 1, wherein said chip is operable, upon said unlocking, to transmit data to a chip reader by way of said communication interface.

4. The chip of claim 3, wherein said transmitted data is transmitted in encrypted form.

5. The chip of claim 3, wherein said transmitted data comprises at least one of a unique identifier of said chip, a unique user identifier, a unique account identifier, a unique mobile service subscriber identifier, a unique transaction identifier, an electronic ticket identifier, a voucher code, and a network authentication code.

6. The chip of claim 5, wherein said unique account identifier comprises a credit card number or a debit card number.

7. The chip of claim 5, wherein said network authentication code comprises at least one of a timestamp and a transaction identifier.

8. The chip of claim 5, wherein said authentication circuit is further operable to update said network authentication code at pre-defined time intervals.

9. A card comprising said chip of claim 1.

10. The card of claim 9, wherein said card is an identity card, a payment card, or an access control card.

11. The card of claim 10, wherein said access control card is for gaining access to at least one of a public transportation service, a particular vehicle, and a particular location.

12. The card of claim 10, further comprising a magnetic stripe storing a network authentication code.

13. The card of claim 9, wherein said card is a SIM card.

14. The card of claim 13, wherein said SIM card is a GSM SIM card, USIM card, a CSIM card, a R-UIM card, a Universal Integrated Circuit Card, a high-capacity SIM card, or a MegaSIM card.

15. The card of claim 13, wherein said card, upon said unlocking said chip, is operable to transmit a message to another SIM card by way of said communication interface of said chip.

16. The card of claim 13, wherein said card, upon said unlocking said chip, is operable to transmit payment data to a point-of-sale terminal by way of said communication interface of said chip.

17. A document comprising said chip of claim 1.

18. The document of claim 17, wherein said document is a passport or a travel visa.

19. An electronic device comprising said chip of claim 1.

20. The device of claim 19, wherein said device is a mobile phone, a tablet, a computer, a set-top box, a television, a Smart TV, a modem, a network switch, a network router.

21. A vehicle comprising said chip of claim 1.

22. The vehicle of claim 21, wherein said vehicle, upon said unlocking said chip, is operable to transmit payment data by way of said communication interface of said chip.

23. A self-authenticating card comprising:

a first chip having a first memory region storing a first authentication code, and a communication interface for communicating with a chip reader; and

a second chip having a second memory region storing a second authentication code;

at least one of said first and second chips providing an authentication circuit interconnected with said first memory region and said second memory region, said authentication circuit operable to:

read said first authentication code from said first memory region;

read said second authentication code from said second memory region;

authenticate said card by comparing said first authentication code with said second authentication code; and

upon said authenticating:

unlock at least one of (i) said communication interface to allow data to be transmitted therethrough (ii) a third memory region to allow data to be read therefrom.

24. The card of claim 23, wherein said communication interface comprises at a radio-frequency transmitter.

25. The card of claim 23, wherein said first chip is operable, upon said unlocking, to transmit data to a chip reader by way of said communication interface.

26. The card of claim 25, wherein said transmitted data comprises at least one of a unique identifier of said chip, a unique user identifier, a unique account identifier, a unique mobile service subscriber identifier, a unique transaction identifier, an electronic ticket identifier, a voucher code, and a network authentication code.

27. The card of claim 25, wherein said transmitted data is transmitted in encrypted form.

28. The card of claim 23, wherein said second chip is substantially sealed within said card.

29. The card of claim 23, further comprising a power source that supplies power to said first and second chips.

30. The card of claim 23, wherein said first and second chips are interconnected by carbon nanowires.

31. The card of claim 23, wherein said card is an identity card, a payment card, an access control card, or a SIM card.

32. An authentication system comprising:

a self-authenticating chip of claim 2 or a self-authenticating card of claim 24; and

a computing device comprising:

a radio-frequency receiver;

a network communication interface;

at least one processor; and

memory interconnected to said at least one processor, said memory storing software code that, upon execution by said at least one processor, causes said computing device to:

receive a network authentication code from said self-authenticating chip or said first chip of said self-authenticating card, by way of said radio-frequency receiver; and

transmit said network authentication code to a network-interconnected authentication server by way of said network communication interface.

33. The authentication system of claim 32, wherein said computing device further comprises a peripheral communication port and said radio-frequency receiver is removably attached to said peripheral communication port.

34. The authentication system of claim 33, wherein said peripheral communication port is a Universal Serial Bus port.

35. The authentication system of claim 32, wherein said computing device is a mobile phone or a tablet computer.

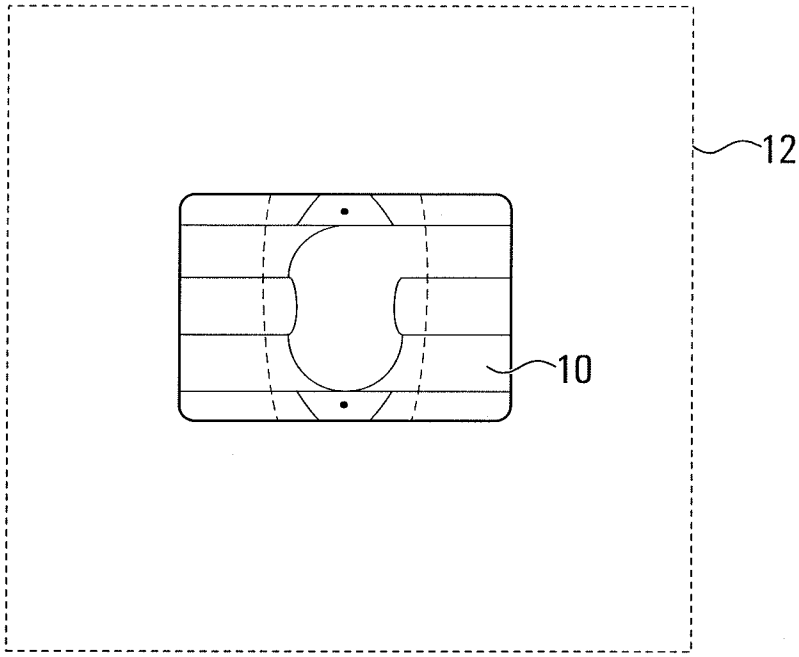


FIG. 1

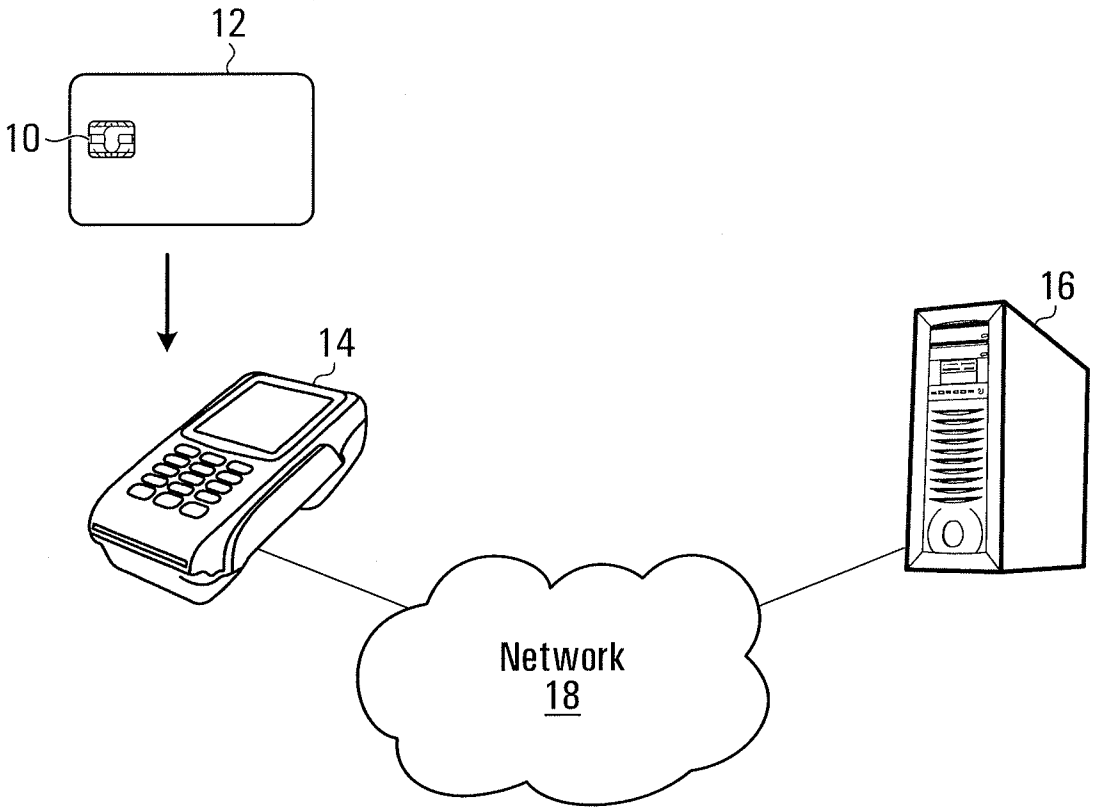


FIG. 2

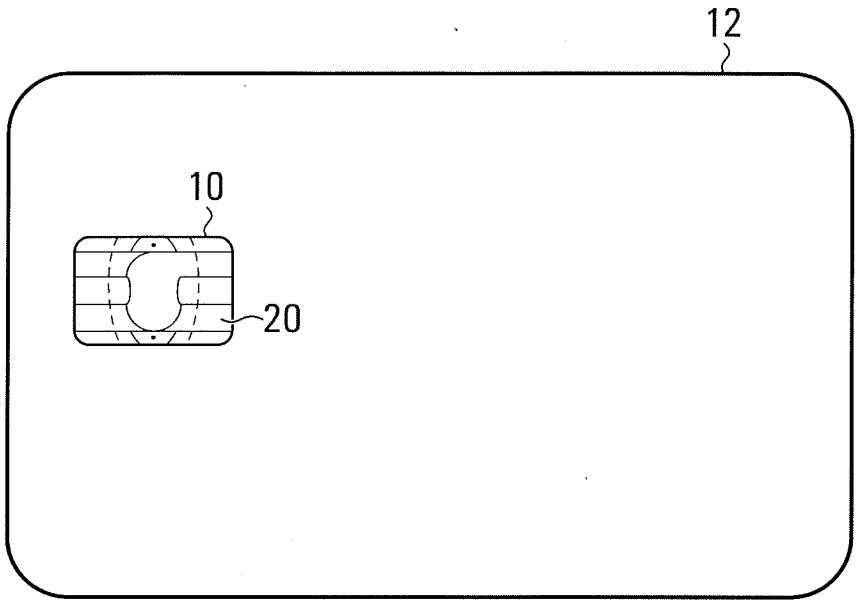


FIG. 3A

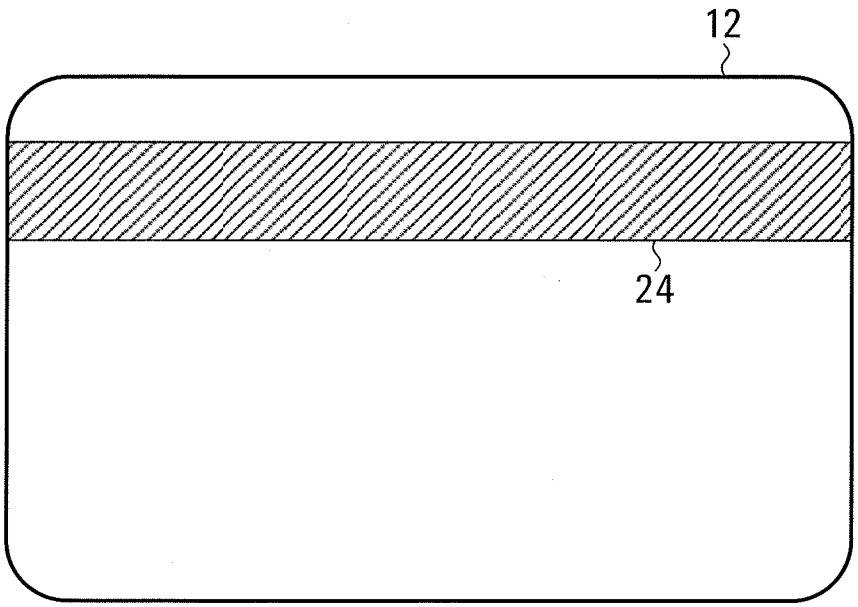


FIG. 3B

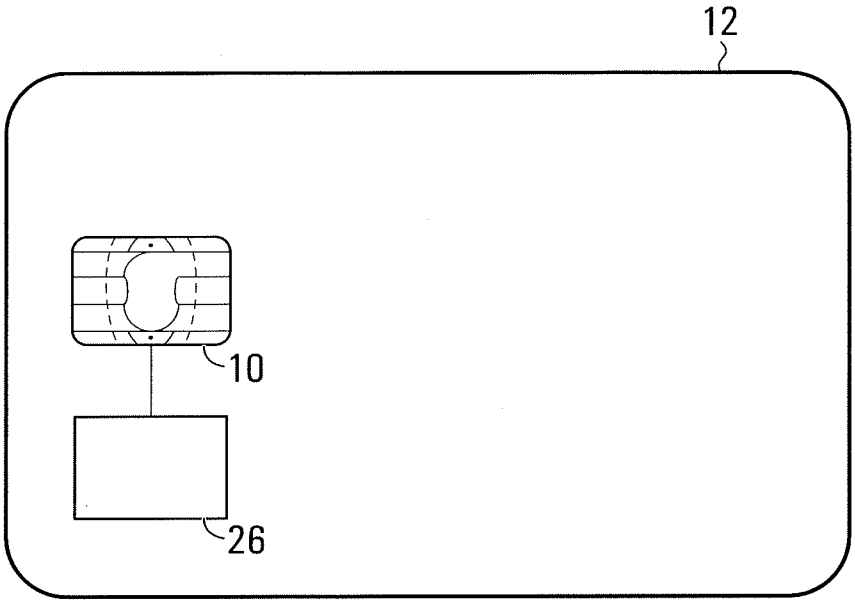


FIG. 3C

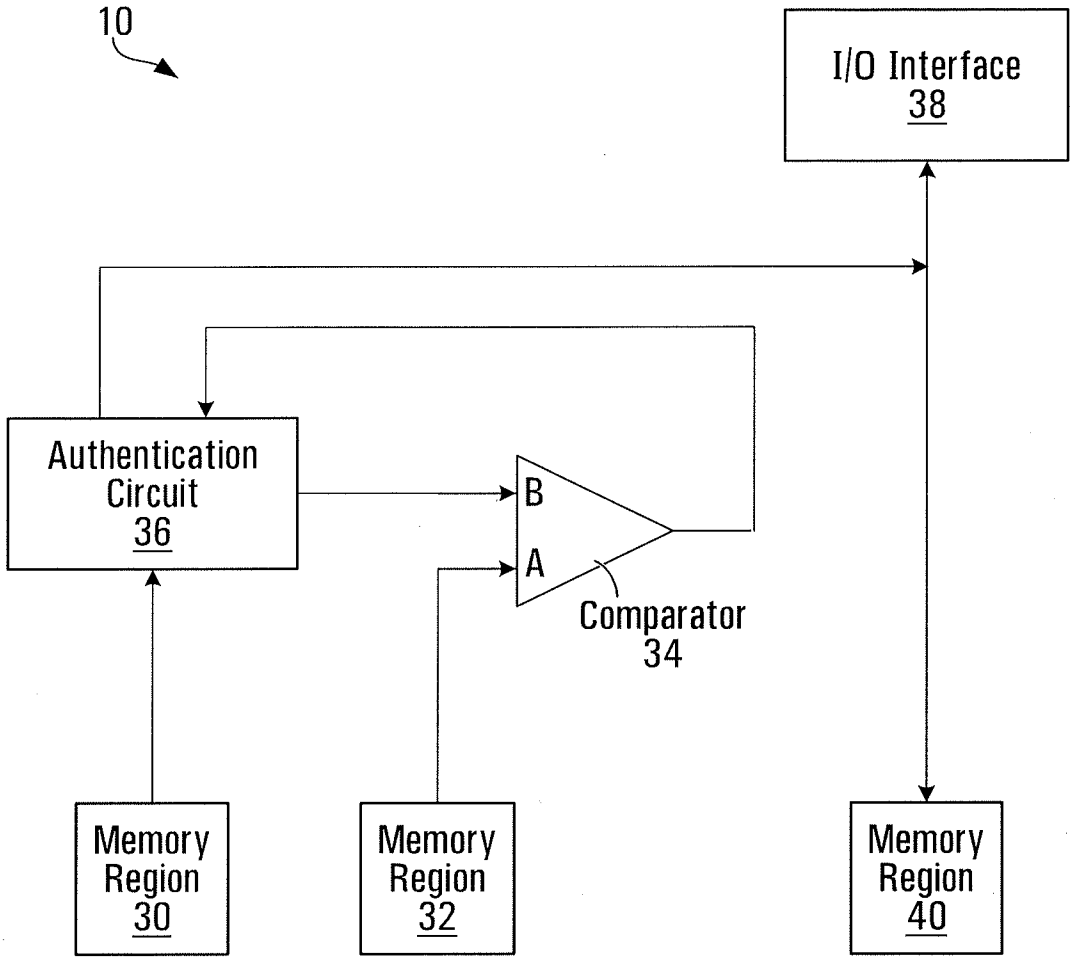

10
I/O Interface
38
Authentication
Circuit
36
B
A
Comparator
34
Memory
Region
30
Memory
Region
32
Memory
Region
40

FIG. 4

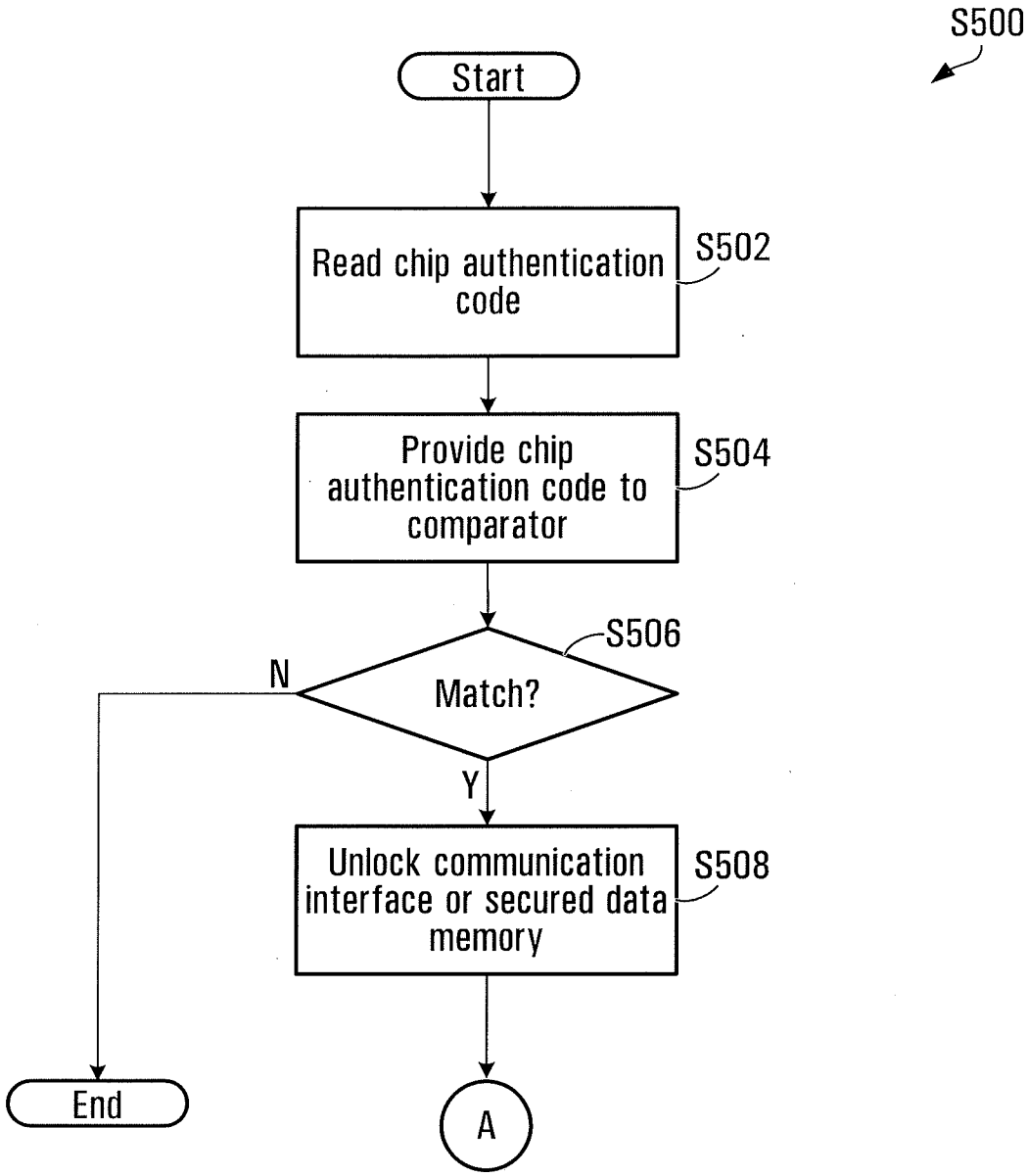

S500
Start
Read chip authentication code
S502
Provide chip authentication code to comparator
S504
S506
Match?
N
Y
Unlock communication interface or secured data memory
S508
End
A

FIG. 5A

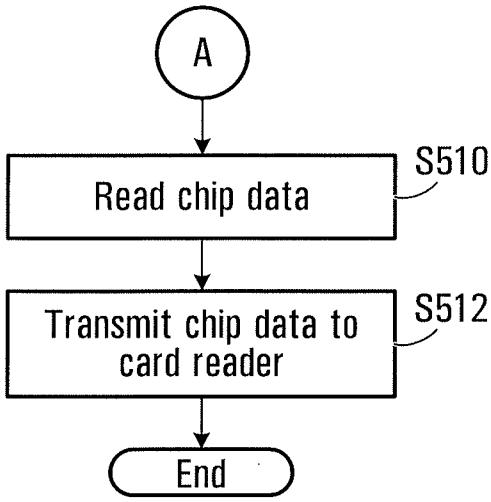

A
Read chip data
S510
Transmit chip data to card reader
S512
End

FIG. 5B

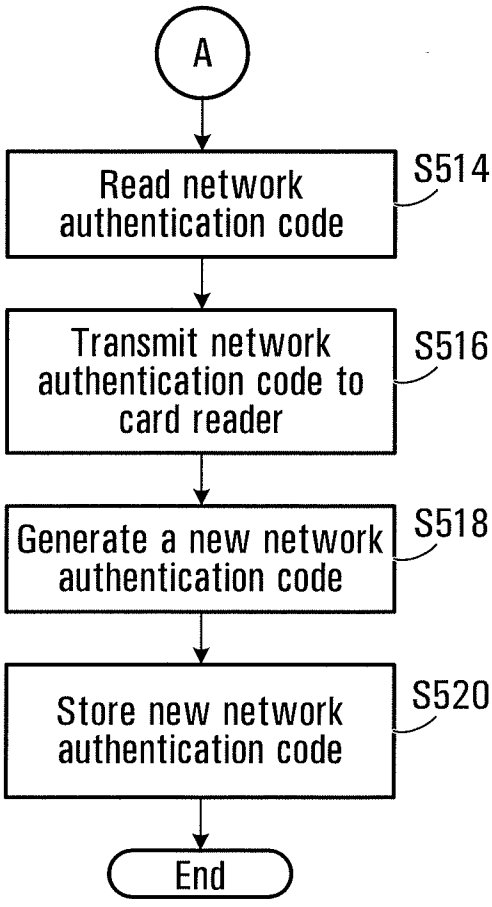

A
Read network authentication code
S514
Transmit network authentication code to card reader
S516
Generate a new network authentication code
S518
Store new network authentication code
S520
End

FIG. 5C

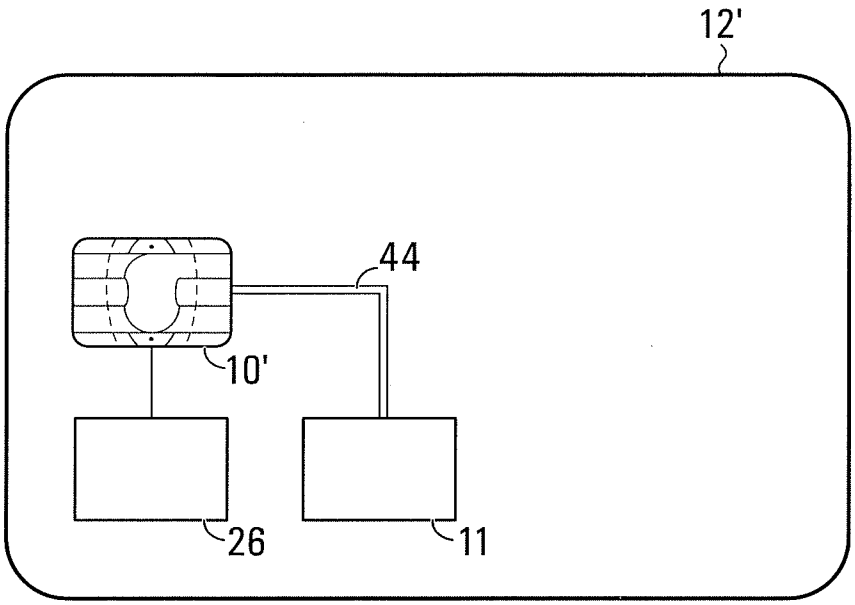


FIG. 6

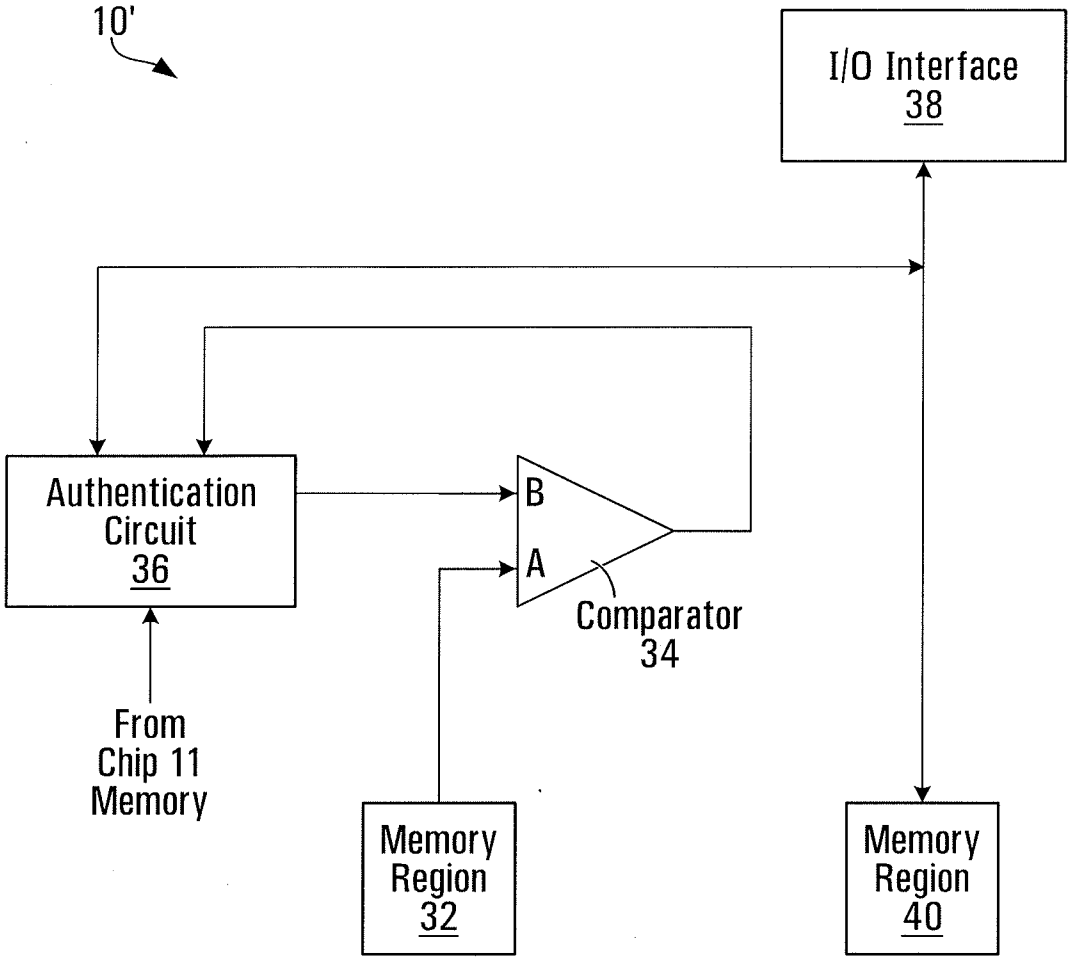

10'
I/O Interface
38
Authentication
Circuit
36
B
A
Comparator
34
From
Chip 11
Memory
Memory
Region
32
Memory
Region
40

FIG. 7

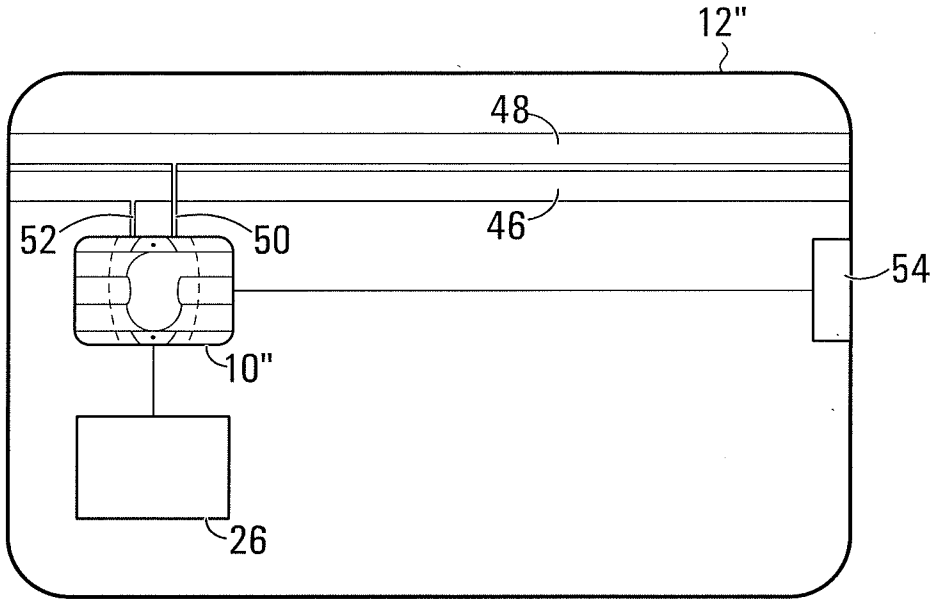


FIG. 8

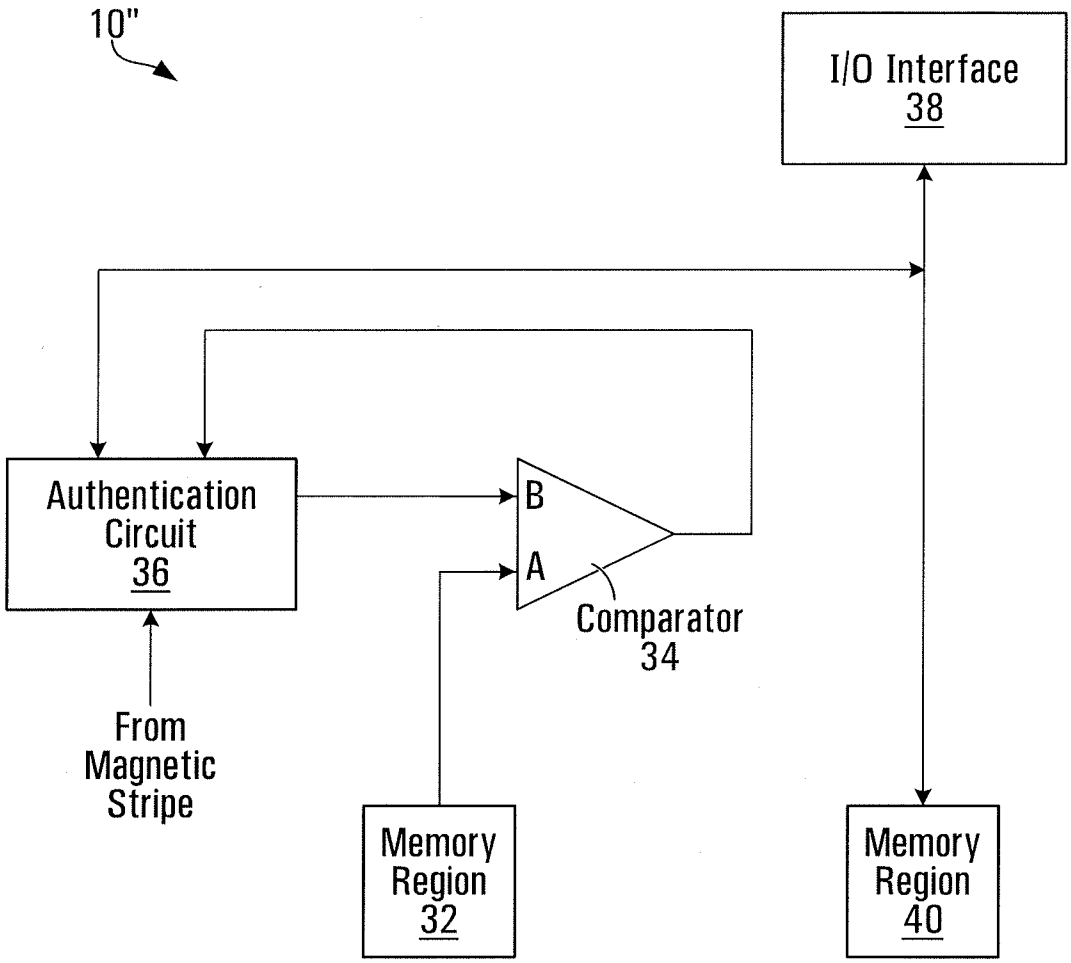

10"
I/O Interface
38
Authentication
Circuit
36
B
A
Comparator
34
From
Magnetic
Stripe
Memory
Region
32
Memory
Region
40

FIG. 9

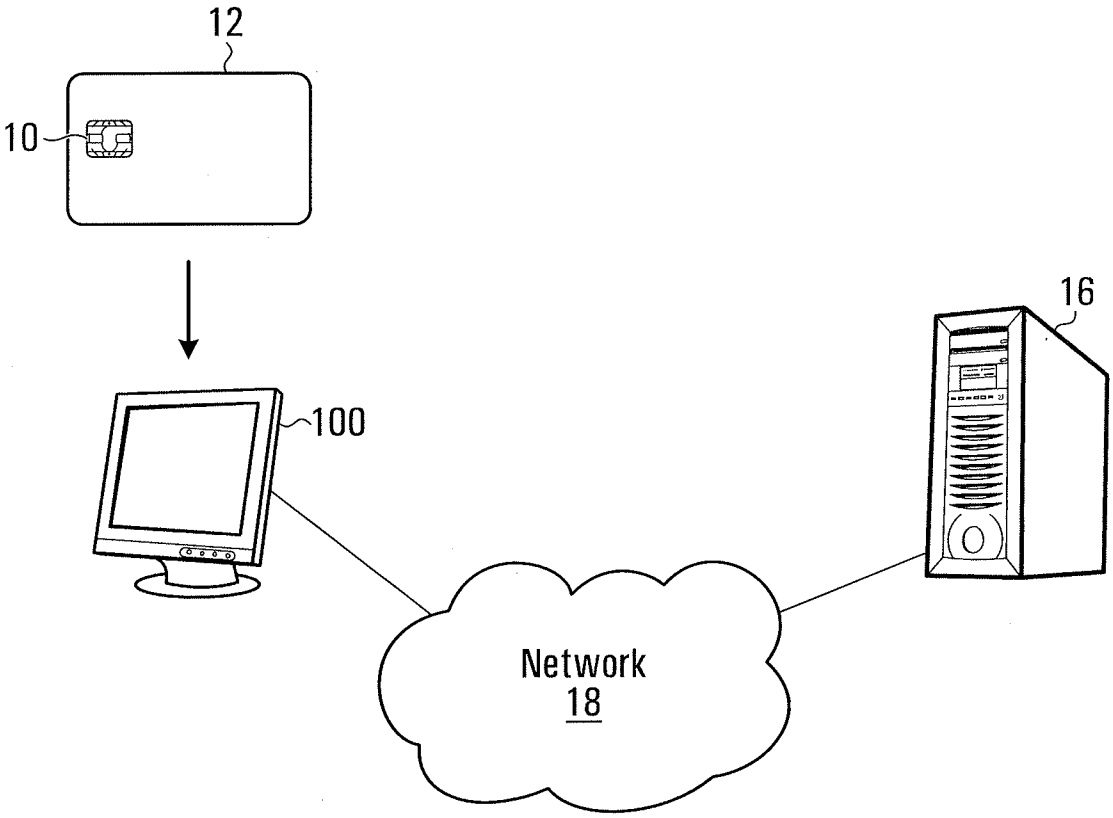


FIG. 10

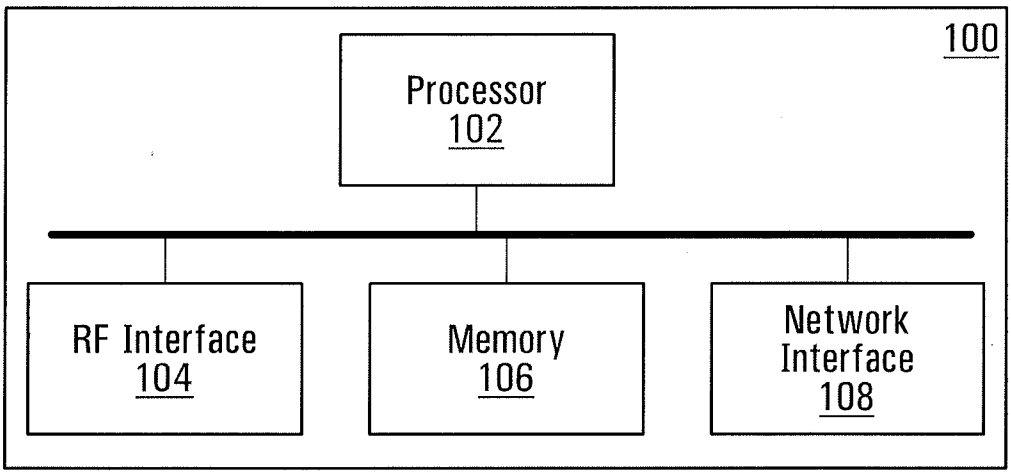

100
Processor
102
RF Interface
104
Memory
106
Network
Interface
108

FIG. 11

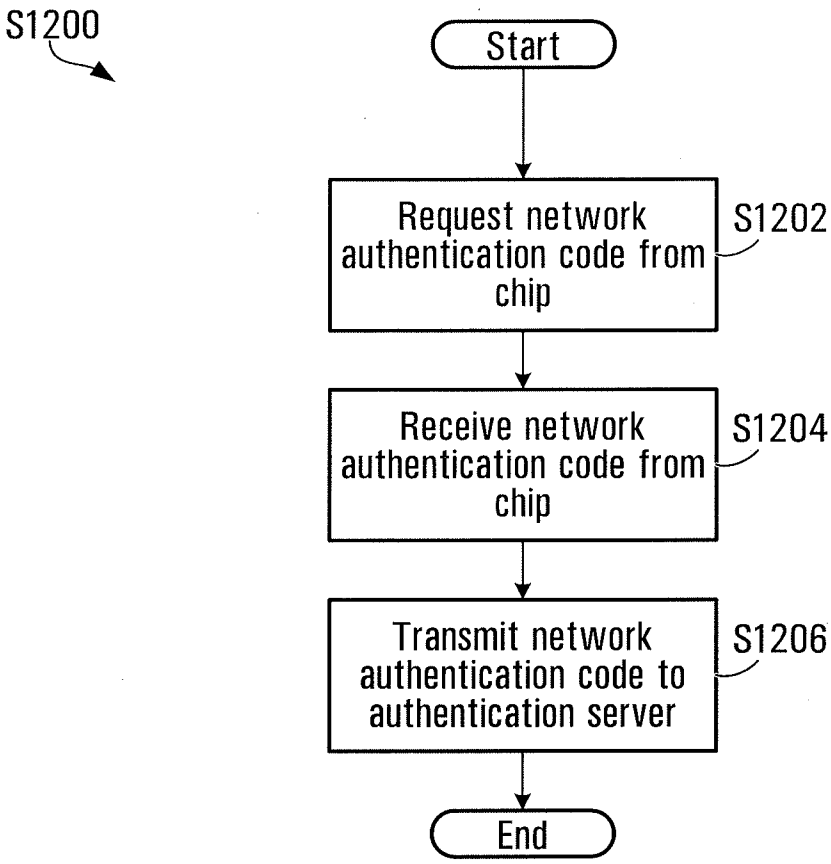

S1200
Start
Request network authentication code from chip
S1202
Receive network authentication code from chip
S1204
Transmit network authentication code to authentication server
S1206
End

FIG. 12

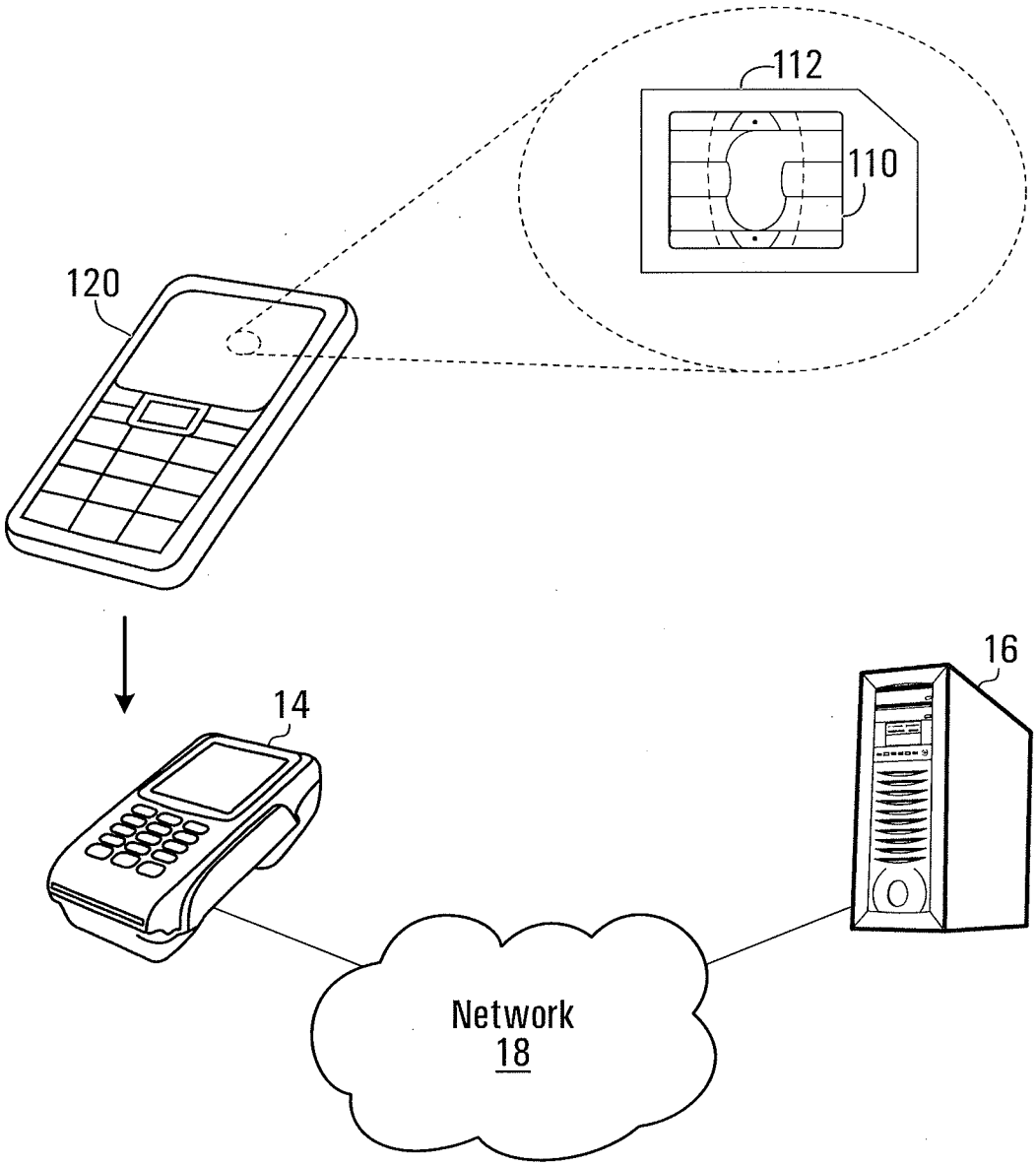


FIG. 13

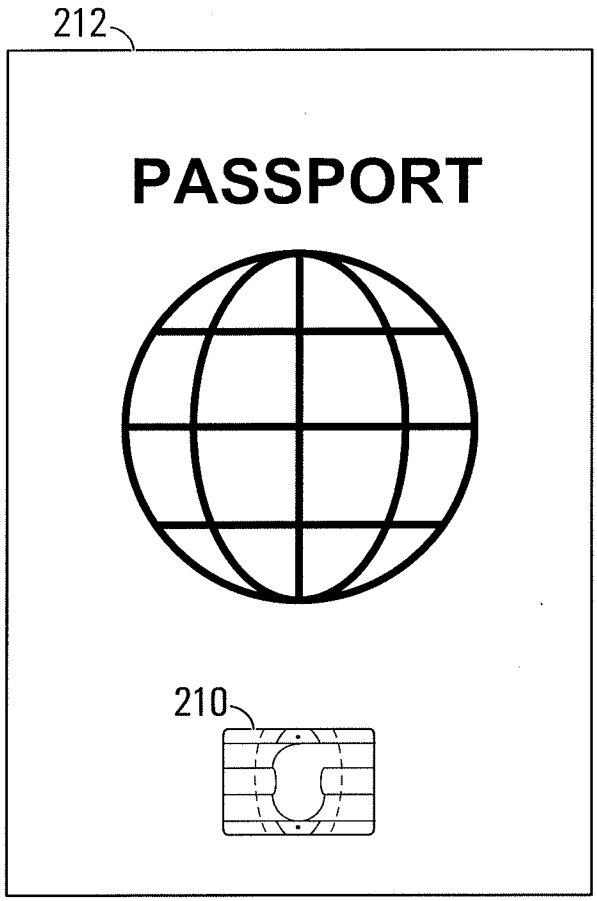


FIG. 14

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2015/050286

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***G06K 19/073*** (2006.01) , ***G06Q 20/34*** (2012.01) , ***G06Q 20/40*** (2012.01) , ***G07C 9/00*** (2006.01)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC: ***all***

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

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Canadian patent database and Questel Orbit
Some search term used: memory, self authenticating chip, self authenticating card, comparator, authentication and code

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2009/0158445 (Dewar) 18 June 2009 (18-06-2009) See entire document	1-35
P, A	US 2014/0165141 (Chellappa et al.) 12 June 2014 (12-06-2014) See entire document	1-35

☐ Further documents are listed in the continuation of Box C.

☑ See patent family annex.

*	Special categories of cited documents:
"A"	document defining the general state of the art which is not considered to be of particular relevance
"E"	earlier application or patent but published on or after the international filing date
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O"	document referring to an oral disclosure, use, exhibition or other means
"P"	document published prior to the international filing date but later than the priority date claimed
"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&"	document member of the same patent family

Date of the actual completion of the international search 18 June 2015 (18-06-2015)	Date of mailing of the international search report 08 July 2015 (08-07-2015)
Name and mailing address of the ISA/CA Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001-819-953-2476	Authorized officer C. Wong (819) 934-2666

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2015/050286

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US2009158445A1	18 June 2009 (18-06-2009)	US8196215B2	05 June 2012 (05-06-2012)
		GB0724422D0	30 January 2008 (30-01-2008)
		GB2455567A	17 June 2009 (17-06-2009)
		GB2455567B	26 December 2012 (26-12-2012)
US2014165141A1	12 June 2014 (12-06-2014)	US9038133B2	19 May 2015 (19-05-2015)
		CN103870742A	18 June 2014 (18-06-2014)
		DE102013224104A1	12 June 2014 (12-06-2014)
		GB201320411D0	01 January 2014 (01-01-2014)
		GB2509823A	16 July 2014 (16-07-2014)