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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2865148 C 2015/06/09

(11)(21) **2 865 148**

(12) BREVET CANADIEN / CANADIAN PATENT

(13) **C**

(86) **Date de dépôt PCT/PCT Filing Date:** 2013/04/17
(87) **Date publication PCT/PCT Publication Date:** 2013/10/24
(45) **Date de délivrance/Issue Date:** 2015/06/09
(85) **Entrée phase nationale/National Entry:** 2014/08/21
(86) **N° demande PCT/PCT Application No.:** AU 2013/000400
(87) **N° publication PCT/PCT Publication No.:** 2013/155563
(30) **Priorités/Priorities:** 2012/04/17 (AU2012901495); 2013/03/22 (AU PCT/AU2013/000299)

(51) **Cl.Int./Int.Cl.** ***H04L 9/12*** (2006.01)

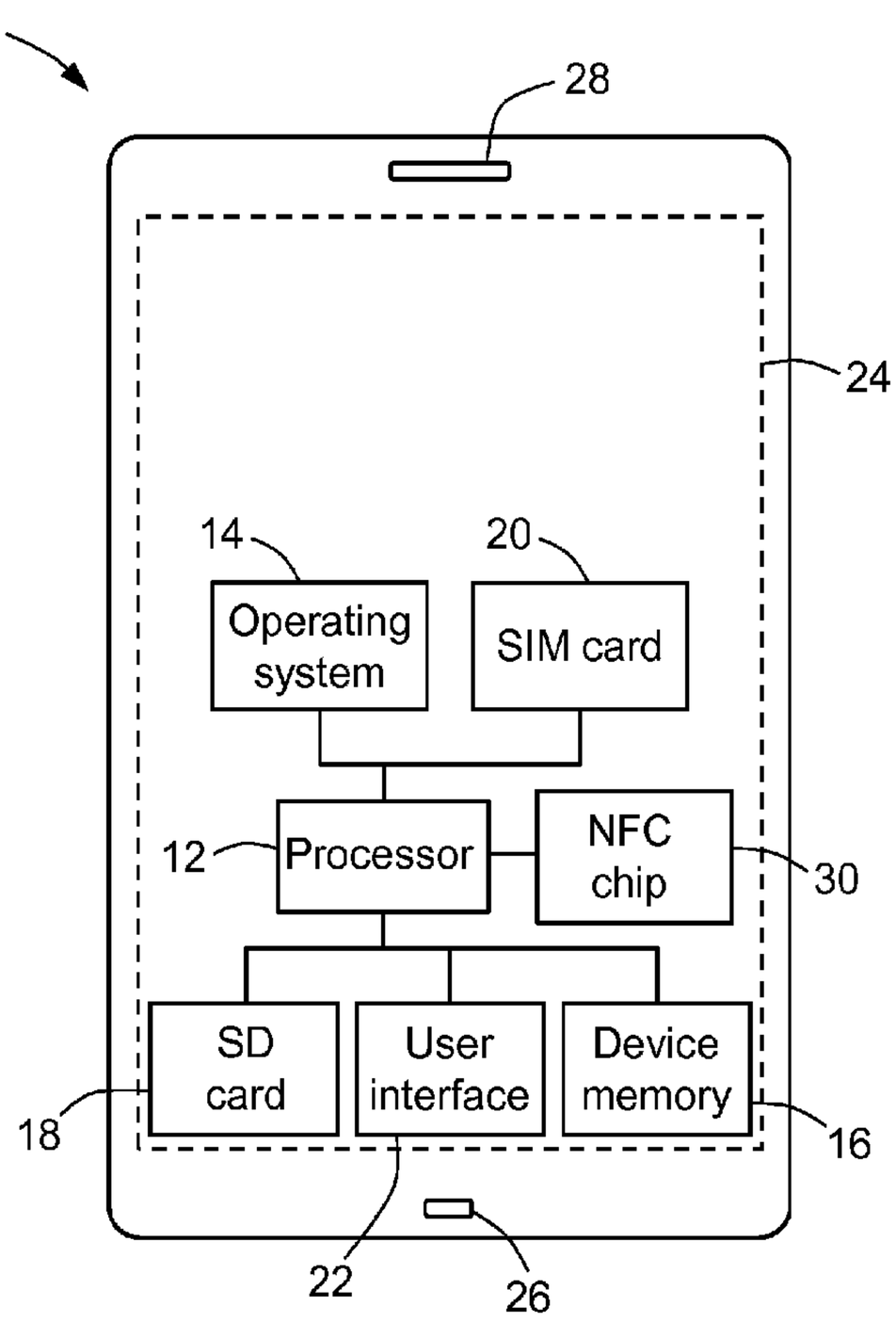
(72) **Inventeur/Inventor:**
NICOLAU, CONSTANTIN M., AU

(73) **Propriétaire/Owner:**
SECURE NFC PTY. LTD., AU

(74) **Agent:** MILTONS IP/P.I.

(54) **Titre : ARCHITECTURE DE PARTITION D'ELEMENTS SECURISES DE MULTIPLES EMETTEURS POUR DES DISPOSITIFS NFC**

(54) **Title: MULTI-ISSUER SECURE ELEMENT PARTITION ARCHITECTURE FOR NFC ENABLED DEVICES**



(57) **Abrégé/Abstract:**
A method for providing secure element partitions for an NFC enabled device for a plurality of card issuers, the method comprising creating in a secure element of the NFC enabled device a plurality of secure element partitions; and allocating said secure element partitions of the secure element to the respective card issuers.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 October 2013 (24.10.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/155563 A1

(51) International Patent Classification:
H04L 9/12 (2006.01)

(21) International Application Number:
PCT/AU2013/000400

(22) International Filing Date:
17 April 2013 (17.04.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2012901495 17 April 2012 (17.04.2012) AU
PCT/AU2013/000299 22 March 2013 (22.03.2013) AU

(71) Applicant: **SECURE NFC PTY. LTD.** [AU/AU]; 450 St Kilda Road, Melbourne, Victoria 3004 (AU).

(72) Inventor: **NICOLAU, Constantin M.**; 10 Birdwood Street, Bentleigh East, Victoria 3165 (AU).

(74) Agent: **GRIFFITH HACK**; GPO Box 1285, Melbourne, Victoria 3001 (AU).

(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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, 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, ML, MR, NE, SN, TD, TG).

Published:

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

(54) Title: MULTI-ISSUER SECURE ELEMENT PARTITION ARCHITECTURE FOR NFC ENABLED DEVICES

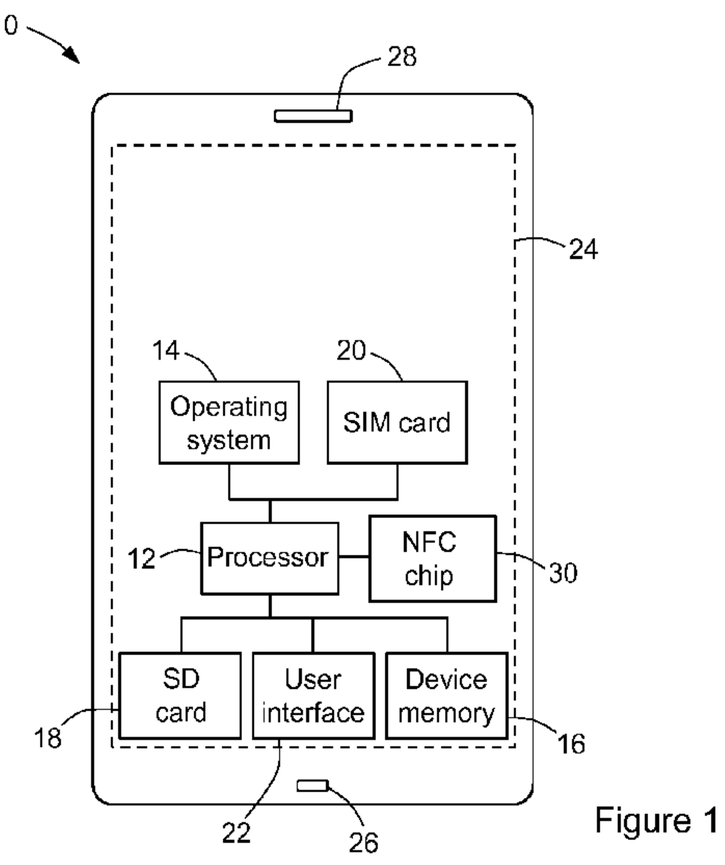


Figure 1

(57) Abstract: A method for providing secure element partitions for an NFC enabled device for a plurality of card issuers, the method comprising creating in a secure element of the NFC enabled device a plurality of secure element partitions; and allocating said secure element partitions of the secure element to the respective card issuers.

WO 2013/155563 A1

Multi-issuer Secure Element Partition Architecture for NFC Enabled Devices

Field of the Invention

The invention relates to the field of information technology security (ITS), and particularly, but not exclusively, to a multi-issuer architecture to enable the coexistence of the Secure Element partitions allocated to each card issuer within NFC enabled devices such as mobile smart-phones.

Background of the Invention

The Near Field Communications (NFC) standard (18000-3) defines the communication protocol between peer to peer NFC active devices and also between NFC active devices and NFC passive "tags" in terms of flow control, message formats, speed (106 Kbs/Miller coding 100% modulation to 424 Kbs/Manchester coding 1% modulation) and frequency (13.56 MHz), but not a methodology for managing multiple Secure Element (SE) partitions.

An SE is a tamper proof (PCI/PED-like) integrated circuit card (ICC) chip/SIM card/micro-SD (Secure Digital) module capable of embedding smart card-grade applications (e.g., payment, ticketing, access control, etc.) security features. The SE is connected to an NFC chip, which acts as a contactless front end radio frequency (RFID) interface and contains among other things the Card-Issuer's security domain Access Control data (used to manage multiple Application Security Domains which in turn contain the Application Developer's security domain Access Control data).

NFC technology provides high data transmission speed, communications protocol simplicity and low cost, but NFC technology has introduced security vulnerabilities that allow, for example: i) eavesdropping by unauthorized parties ('snooping'), data modification or insertion, ii) data manipulation, corruption and insertion by impersonators ('phishing'), and iii) denial of service ('jamming') and virus attacks by supposedly trusted parties.

To protect the NFC data exchange, processing and storage privacy and integrity, the major Card Issuers have formed alliances with either the mobile operating systems developers or the NFC device manufacturers, and implemented proprietary proof-of-end point protocols using public key signatures and message encryption and authentication.

However, an NFC enabled device (such as a smart-phone) is generally the property of—or at least for the exclusive use of—an individual consumer. Such a consumer may have multiple credit cards, electronic wallets or the like provided by a plurality of financial or other institutions, but the current dedicated security solutions and SE management methodologies do not permit the existence of multiple SE on the same NFC enabled device.

Summary of the Invention

According to a first broad aspect of the invention, there is provided a method for providing secure element partitions for an NFC enabled device for a plurality of card issuers, the method comprising:

creating in a secure element (and in some cases in more than one secure element) of the NFC enabled device a plurality of secure element partitions; and

allocating said secure element partitions of the secure element (or secure elements) to the respective card issuers.

The method may include creating or locating in a memory of the NFC enabled device the secure element (or secure elements).

It will be appreciated that in some cases a secure element or elements will already have been created in the NFC enables device, and hence the method may merely have to locate that secure element in order to then create in the secure element(s) the secure element partitions.

The method may include one or more of the card issuers loading secure element data and programs (which may be authenticated/certified and signed) into the respective secure element partitions allocated to the respective card issuers.

For example, the card issuer's data may be loaded as a part of an Acquirer Group's Virtual Wallet, on any NFC enabled device managed by the respective Transaction Acquirer/Processor or Trusted Service Manager (TSM).

The method may include creating 8, 16 or 32 (or more) of the secure element partitions in the at least one secure element.

The method may include allocating the secure element partitions to respective cards of the respective card issuers.

The method may include creating in at least one of the secure element partitions a plurality of application security domains for storing respective software applications.

The method may include creating 2, 4 or 8 (or more) of the application security domains for one or more of the card issuers.

The method may include providing in the secure element partitions respective sets of one or more cryptographic keys, wherein each of the sets of cryptographic keys is unique to one of the card issuers.

In one embodiment, each of the sets of cryptographic keys comprises 256 random byte keys. Each of the keys may comprise 8 bits. Indeed, each of the keys may comprise an ASCII character.

The memory may be in a SIM card of the device, a micro-SD of the device or a cache of the device.

The method may include providing a secure element partition loader, secure element partition manager, and a secure element partition cryptographic module in the NFC enabled device for implementing the method.

According to this aspect of the invention, there is also provided an NFC enabled device provided with secure element partitions according to the above-described method.

According to a second broad aspect of the invention, there is provided NFC enabled device, comprising:

a secure element comprising a plurality of secure element partitions;

a secure element partition loader for updating or loading executable code and data into each of the secure element partitions; and

a secure element partition manager for identifying and selecting one of the secure element partitions allocated to a specific card issuer;

wherein each of the secure element partitions has a security domain comprising an access rule application master having access rules and cryptographic keys; and

the NFC enabled device further comprises a secure element partition cryptographic module for controlling access to the respective security domains of the secure element partitions.

According to a third broad aspect of the invention, there is a provided computer program product that, when executed on a computer:

creating in at least one secure element (and in some cases in more than one secure element) of the NFC enabled device a plurality of secure element partitions; and

allocates said secure element partitions of the secure element to the respective card issuers.

The computer program product may also create or locate in a memory of the NFC enabled device the at least one secure element.

The computer program product may also create in at least one of the secure element partitions a plurality of security domains for storing respective software applications or data or both software applications and data.

According to a fourth broad aspect of the invention, there is provided a computer readable storage medium with a computer program product according to the third broad aspect.

It should be noted that any of the various individual features of each of the above aspects of the invention, and any of the various individual features of the embodiments described herein including in the claims, can be combined as suitable and desired.

Brief Description of the Drawing

In order that the invention may be more clearly ascertained, embodiments will now be described, by way of example, with reference to the accompanying drawing, in which:

Figure 1 is a schematic block diagram of an NFC enabled smartphone according to an embodiment of the present invention;

Figure 2 is a schematic block diagram of some of the operational components of the operating system and the micro-SD of the smartphone of figure 1;

Figure 3 is a schematic block diagram of the operating system and the micro-SD of the smartphone of figure 1 and their relationship to the systems of various external parties;

Figure 4 is a schematic block diagram of the architecture of the smartphone of figure 1; and

Figure 5A is a flowchart of the installation of program modules embodying the present invention into the smartphone of figure 1;

Figure 5B is a flowchart of the use of the program modules embodying the present invention into the smartphone of figure 1; and

Figure 6 is a schematic block diagram of the architecture of the multi-issuer SE partition manager of the operating system of the smartphone of figure 1.

Detailed Descriptions of the Figures

Figure 1 is a schematic block diagram of an NFC enabled device, in this example a smartphone 10, according to an embodiment of the present invention. For clarity, only features are particular relevance to understanding the present invention are illustrated in the figure and described below.

Smartphone 10 includes a processor 12, an operating system 14 (e.g. Android (trade mark), iOS (trade mark), Symbian (trade mark), BlackBerry OS (trade mark) or Windows 8 (trade mark)), and two forms of memory: device memory 16 and a removable micro-SD (secure digital) memory card 18 (hereafter 'micro-SD 18'). In addition, smartphone 10 includes a SIM card 20, which has some on-board memory, and a user interface shown schematically at 22, but which includes a touch screen 24, microphone 26 and speaker 28. Smartphone 10 also includes an NFC chip 30.

Figure 2 is a schematic block diagram of some of the operational components of operating system 14 and micro-SD 18 according to the present embodiment. Operating system 14 includes an operating system (OS) kernel 30, which includes one or more device applications 32 (of which only a first exemplary device application is shown for clarity), an application manager 34, utility services module 36, communications services module 38 and an secure element (SE) access API 40. Each device application 32 includes a digital signature 42 and a digital certificate 44, and is in data communication with application manager 34, utility services module 36 and communications services module 38. SE access API 40 includes an access control enforcer 46 (an API defined by GlobalPlatform (trade mark)), and program modules that implement various functions of the present embodiment, including an SE partition

manager 48, whose main role is to identify and select the SE partition allocated in a specific card to a specific card issuer, an SE partition loader 50, whose main role is to either update (or replace) or load executable code and data (rules, SCST, etc.) into the selected SE partition, and an SE partition cryptographic module 52, whose main role is to ensure only authorized access to the security domain (SD) access rules and SCST loaded into the selected card issuer's ARA-M of the specific SE partition.

Micro-SD 18 includes one or more multi-partition secure elements (SEs) 60 (of which only a first exemplary multi-partition SE is shown for clarity). Each multi-partition SE 60 is partitioned into a plurality of secure element (SE) partitions 62(1), 62(2),..., 62(n); each SE partition 62(1), 62(2),...62(n) is allocated to a respective card-issuer 1, 2,..., n. In this embodiment, each SE 60 has—in this embodiment—8, 16 or 32 SE partitions 62(1), 62(2),..., 62(n).

Each SE partition 62(1), 62(2),..., 62(n) has an access rule application master (ARA-M) 64 that includes, in the example of SE partition 62(1), a first register 66 that stores access rules and control data of the respective card issuer and a second register 68 that stores a unique smart-card security table (SCST) of random keys generated by the respective card issuer to protect that card issuer's NFC cards. Each SE partition 62(1), 62(2),..., 62(n) also has an SCST version no. register (indicated at 69 for SE partition 62(1)) with the SCST version number used by the respective card issuer. Each NFC card released by a card issuer is initialized with the unique SCST in the second register of that card issuer, so each NFC device is loaded with the respective SCSTs and SCST version numbers associated to the NFC cards expected to be used with the device (in this example, smartphone 10).

Each card issuer can thus stipulate, with its respective access rules and control data, its own set of access rules for the management and control of data in its dedicated SE partition within the multi-partition SE 60. Access control enforcer (ACE) 46 of operating system 14 controls access to ARA-M 64.

The SCST in each SE partition 62(1), 62(2),..., 62(n) holds different sets of security keys for securing the data in each respective SE partition 62(1), 62(2),..., 62(n). Any suitable technique may be employed to generate security keys, but in this embodiment each SCST is generated—by the respective card issuer—and employed using implicit key management (IKM) module 70, according to the IKM method disclosed in Australian patent application no. 2012901149 filed 22 March 2012 and international

patent application no. PCT/AU2013/000299 filed 22 March 2013. Thus, the SCST in SE partition62(1) contains 256 random byte keys of 8 bits each, employed to encrypt/decrypt datastored in the respective SE partition as described in those patent applicationsaccording to IKM module 70 to provide data integrity, privacy and non-repudiation formessages exchanged with other active (peer smart-phones, EFTPOS and otherdevices) or passive devices (such as contact and contactless smart-cards and TAGs).The other SE partitions contain comparable SCSTs, with different sets of keys.

In addition, each SE partition 62(1), 62(2), ..., 62(n) can use one or more application security domains (SDs). Each application SD on a particular SE partition 62(1), 62(2),..., 62(n) may contain an application authorized by the card issuer to which the corresponding SE partition is allocated; each application is provided by a respective application provider.

Figure 2 depicts examples of application SDs 72(1), 72(2),..., 72(i) associated with SE partition 62(1) of card issuer 1, but it will be understood that each of SE partitions 62(1), 62(2),..., 62(n) may have none, one or more than one application SDs. In this embodiment, each SE partition 62(1), 62(2), ...,62(n) contains 2, 4 or 8 application SDs 72(1), 72(2),..., 72(i) and hence generally 2, 4 or 8 applications (though in other embodiments there may be more application SDs per SE partition and hence correspondingly more applications). As with the number of card issuer SE partitions per SE, the number of application SDs per card issuer SE partition is limited by the memory size of the medium used to store the SEs, in this example micro-SD 18, and it is envisaged that greater numbers of card issuer SE partitions per SE and of application SDs per card issuer SE partition will be possible as the memory size of available media increases.

Application SD 72(1) of SE partition 62(1) is described below as an example, but the other application SDs of SE partition 62(1) have comparable features (though different respective applications). In this example, the application stored in application SD 72(1) is Cyber Security Shield (CSS) 74, an application for protecting the contents of NFC and other smart-cards as well as the communications between such smart-cards and NFC enable devices in terms of data integrity, privacy and non-repudiation. Application SD 72(1) also includes an access rule applications client (ARA-C) 76 that is managed by ARA-M 64 of card issuer SE partition 62(1), and an application register 77 that contains the IDs of any other card issuers that share the application (CSS 74) with the

card issuer to whom SE partition 62(1) is allocated. ARA-C 76 includes a set of access rules and control data 78.

Application register 77 of shared applications (and the corresponding application registers in the other application SDs) are maintained by SE partition manager 48. As mentioned above, these application registers include data indicative of the other authorized card issuers, so that access control enforcer 46, which—as described above—controls access to ARA-M 64 of SE partition 62(1) and to the ARA-Ms of the other card issuer SE partitions, can ensure that only authorized (other) card issuers can use such applications.

In this example, application SD 72(2) of SE partition 62(1) contains EMV (which stands for 'Europay, MasterCard, Visa'), an application that provides enhanced security for credit and/or debit payment smart-cards. Application SD 72(2) includes its own access rule applications client (cf. ARA-C 76 of application SD 72(1)) that includes a set of access rules and control data and that is also managed by ARA-M 64 of card issuer SE partition 62(1), and an application register (cf. application register of application SD 72(1)) that contains the IDs of the card issuers that share this application with the card issuer to whom SE partition 62(1) is allocated.

One or more additional application SDs may be created for further applications as desired.

In this embodiment, SEs 60 are contained in micro-SD 18, but they may in other embodiments be located on SIM card 20, in a device cache (such as in device memory 16) or in some other PCI PED security module.

Figure 3 is a schematic block diagram of operating system 14 and micro-SD 18 and their relationship to the systems of various parties, such as the card issuers, and the program modules (indicated by 'APP' in the figure) according to the present embodiment—including SE partition manager 48, SE partition loader 50 and SE partition cryptographic module 52. Referring to figure 3, it will be noted that a controlling authority (CA) 80 issues certificates to NFC application provider 82 that provides the program modules (and who receive them from an NFC application developer or owner 84). The NFC application provider 82 provide the program modules, certificates and cryptographic keys (for the SCST in second register 68) to NFC enables devices via a device transaction acquirer (which performs SSD

management) or card enabler 86, under the control of a NFC card issuer 88 (which also gives authority to NFC application developer or owner 84 of the program modules).

Figure 4 is a schematic block diagram 90 of the software architecture of smartphone 10, and the integration of an SE 60 generated by a card issuer with operating system 14. The execution of various NFC security functions is transparent to smartphone 10 and card users. The proprietary NFC Security API enables applications such as business application 92 resident in smartphone 10 to perform the cryptographic functions required to provide data integrity, privacy and non-repudiation.

Figures 5A and 5B are flowcharts 100, 102 of the installation and use, respectively, of the program modules that constitute the embodiment of figures 1 to 3, by reference to smartphone 10; flowcharts 100, 102 describe how new SE partitions within SE 60 are allocated to new card issuers or replaced for existing card issuers, and how the SE partition particulars (data, programs, etc.) are used to protect messages exchanged with third party active or passive devices.

Flowchart 100 of figure 5A shows how NFC devices such as smartphone 10 are loaded with a unique SCST for each card issuer and with the program modules that implement the embodiment of figures 1 to 3, which constitute an NFC security software product for protecting smartphone 10 against security attacks, and how each of SE partitions 62(1), 62(2),..., 62(n) allocated to the card issuers are used to process incoming and outgoing messages between smartphone 10 and either an NFC card or another NFC enabled device. Flowchart 102 of figure 5B illustrates the use of a card issuer's SE partition (*viz.* SE partition 62(1), 62(2),... or 62(n)).

Referring to flowchart 100 of **figure 5A**, the SCST and the aforementioned program modules are downloaded either in-house by the equipment manufacturer (of smartphone 10, of micro-SD 18 or—if SE 60 is to be installed in the SIM card rather than the micro-SD—SIM card 20), supervised by the card issuer, or remotely by selected transaction acquirers (processors). At steps 104, therefore, the program modules for creating and managing a card issuer SE partition of card issuer 'm' (referred to in this figure collectively as the 'SE APP' for a notional card issuer 'm') are loaded onto the micro-SD 18 and, at step 106, the signature and certificate of the SE APP of card issuer 'm' are validated. These two operations can be performed by standard functions of any NFC enabled device that is adapted to validate the source

(proof-of-end-point) and the certificates of any application loaded into the device via any type of interface (e.g. Wi-Fi, NFC, WAN, LAN) or from any medium (e.g. SIM, SAM, micro-SD, memory cache).

At step 108, the SE APP of card issuer 'm' is installed in order to provide secure functions for the card issuer SE partition of SE 60. At step 110, SE partition loader 50 checks the card issuer ID to determine whether the card issuer is an existing card issuer (i.e. an SE partition has already been allocated in SE 60 to card issuer 'm') or a new card issuer.

If SE partition loader 50 determines that the card issuer ID is indicative of an existing card issuer, processing continues at step 112, where the SE APP replaces old SE contents (applications, rules, SCST, etc.) of card issuer 'm' with a new ones and, in doing so, applies strict version control, such that the new version must have a higher version number that the current version stored in second register 68 of the SE partition allocated to card issuer 'm'. Processing then passes to step 114, where a job completion message is displayed by an activity reporting program, then processing ends.

If SE partition loader 50 determines at step 110 that the card issuer ID is indicative of a new card issuer, processing continues at step 116, where SE partition loader 50 determines whether SE 60 has sufficient memory space to allocate a new SE partition to card issuer 'm'. If not, processing continues at step 114, where a job completion message is displayed by an activity reporting program (which indicates insufficient space), then processing ends. If at step 116 SE partition loader determines that SE 60 has sufficient memory space, processing continues at step 118, where SE partition loader 50 allocates a new SE partition in SE 60 to card issuer 'm'. Second register 68 is updated with the version control number of the card issuer's SCST. Subsequently, at step 120, one or more new card issuer authorized applications, once validated, can be loaded into the SE partition of SE 60 allocated to card issuer 'm' if in each case sufficient memory space is available for that new card issuer. Processing then passes to step 114, where a job completion message is displayed by an activity reporting program, then processing ends.

Flowchart 102 of **figure 5B** illustrates the operation of an exemplary read/write application that is configured to issue NFC commands. At step 130 the NFC card data is read and SE partition manager 48 determines the card issuer ID from the card prefix

of the NFC card's personal account number (PAN). At step 132, SE partition manager 48 initiates the read/write application which, at step 134, checks whether it has been passed a read command or a write command.

If a write command is detected, processing continues at step 136 where the read/write application selects the corresponding SE partition allocated to the identified card issuer. The NFC card Write function requires that the data to be written be authenticated and encrypted before its transmission to the NFC card. Using the card issuer's SCST in second register 68, at step 138 the program modules generate a set of implicit keys and the associated vectors. At step 140 the message is encrypted by the newly generated ENCRYPT key 1 and at step 142 authenticated by the AUTH key 2. At step 144 the encryption and authentication keys are destroyed, and at step 146 the message is build by prefixing encrypted and authenticated message with the vectors associated with the implicit keys. At step 148, the resulting message is sent (*viz*. written) onto micro-SD 18 (or, in other examples, written to another NFC card or memory storage, or sent (posted) to a peer NFC enabled device). Processing then ends.

If, at step 134, the read/write application determines that it has been passed a read command, processing continues at step 150, where the read/write application selects the corresponding SE domain allocated to the identified card issuer. Next, at step 152 the NFC card Read function uses the vectors attached to the message/record to regenerate the implicit key used to encrypt and authenticated the message. Once the DES/3DES keys (CRYPTO and AUTH) have been regenerated, at step 154 the message is decrypted using CRYPTO key 1 and at step 156 the message authenticity is verified using AUTH key 2 for its integrity. At step 158, the message contents are processed (viz. read) and at step 160 the keys and the vectors are destroyed. Processing then ends.

Thus, an NFC enabled device may select, under the control of resident ACE 46, the correct card issuer partition upon being presented with a valid PAN or when a virtual card is selected from the card/method of payment menu by the user, as follows:

LOOK PAN prefix (Card-Issuer Prefix Table)
COMPARE PAN prefix range
{YES} ACCESS CI-SE domain (i.e. partition)
{NO} Invalid PAN, EXIT

Signed and certified data and programs may be loaded into card issuer partitions, and maintained, upon the validation of the sender identity and the authentication of the received data contents proceed, as follows:

POEP UNSIGN (Signed CI-ID)
COMPARE CI-ID value (Card-Issuer Prefix Table)
{YES} Authenticate Certificate (CA)
{YES} Authenticate Message (MAC),
{YES} Decrypt Message (DATA, Programs)
Store DATA and/or Programs in CI-SE, EXIT
{NO} Invalid CI-ID, or CA or MAC, EXIT

The contents of the Card-Issuer's partition may be decrypted prior to the use of the specific card issuer's information and data may be encrypted and written back into the card issuer's partition, as follows:

Write Card/Record Process
DECRYPT CI-SE contents using Implicit Key Management
GENERATE random# to create Card Code Factor (CCF)
ENCIPHER data message using CCF key,
WRITE to NFC card, EXIT

Read Card/Record Process
DECRYPT CI-SE contents using Implicit Key Management
GET random# (challenge) to create Card Code Factor (CCF)
DECIPHER data message using CCF key, EXIT

Figure 6 is a schematic block diagram 170 of the architecture of the multi-issuer SE partition manager 48 of operating system 14, according to this embodiment. Access control enforcer 46 uses the services of SE partition manager 48 to manage the loading, maintenance, access and usage of each individual card issuer's SE partition in smartphone 10.

In this embodiment, the size of the SCST in second register 68 of SE partition 62(1) is only 256 bytes and the software components of this embodiment that implement the present invention are of small size in executable form (of the order of 1 KB) and shared by all SE partitions. As discussed above, application register 77 holds merely a list of the card issuers' IDs and levels of authority (execute, update, delete) for the sharing of specific applications in application SD 72(1). Consequently, the memory space

required by this embodiment is very small compared to the memory space of micro-SD 10 (i.e. 32 GB) or of device memory 16 (i.e. 16 GB) of smartphone 10, or even when compared to NFC active cards (which commonly have at least 8 KB).

Modifications within the scope of the invention may be readily effected by those skilled in the art.

For example, it will be apparent to the skilled person in this art that embodiments of the present invention have applications in many instances where secure data storage and security of communications between two NFC devices is required, and that numerous alterations and modifications can be made to the security method and architecture of the above-described embodiments, without departing from the basic concepts of the invention and should be considered within its scope. It is to be understood, therefore, that this invention is not limited to the particular embodiments described by way of example hereinabove.

In the claims that follow and in the preceding description of the invention, except where the context requires otherwise owing to express language or necessary implication, the word “comprise” or variations such as “comprises” or “comprising” is used in an inclusive sense, that is, to specify the presence of the stated features but not to preclude the presence or addition of further features in various embodiments of the invention.

Further, any reference herein to prior art is not intended to imply that such prior art forms or formed a part of the common general knowledge in any country.

CLAIMS:

1. A method for providing secure element partitions for an NFC enabled device for a plurality of card issuers, the method comprising:

creating in a secure element of the NFC enabled device a plurality of secure element partitions; and

allocating said secure element partitions of the secure element to the respective card issuers.

2. A method as claimed in claim 1, including creating or locating in a memory of the NFC enabled device the secure element.

3. A method as claimed in either claim 1 or 2, including one or more of the card issuers loading secure element data and programs into the respective secure element partitions allocated to the respective card issuers.

4. A method as claimed in any one of claims 1 to 3, including creating 8, 16 or 32 of the secure element partitions in the at least one of the secure elements.

5. A method as claimed in any one of claims 1 to 4, including allocating the secure element partitions to respective cards of the respective card issuers.

6. A method as claimed in any one of claims 1 to 5, further comprising creating in at least one of the secure element partitions a plurality of security domains for storing respective software applications or data or both software applications and data.

7. A method as claimed in claim 6, including providing a first of said plurality of security domains with a security application and security data.

8. A method as claimed in any one of claims 1 to 5, further comprising creating in each of the secure element partitions a plurality of security domains for storing respective software applications or data or both software applications and data, including providing in a first of said plurality of security domains of each of said secure element partitions with a security application and security data.

9. A method as claimed in any one of claims 6 to 8, including creating 2, 4 or 8 of the security domains for one or more of the card issuers.

10. A method as claimed in any one of claims 1 to 9, including providing in the secure element partitions respective sets of one or more cryptographic keys, wherein each of the sets of cryptographic keys is unique to one of the card issuers.

11. A method as claimed in claim 10, wherein each of the sets of cryptographic keys comprises 256 random byte keys.

12. A method as claimed in either claim 10 or 11, wherein each of the keys comprises 8 bits.

13. A method as claimed in any one of claims 10 to 12, wherein each of the keys comprises an ASCII character.

14. A method as claimed in any one of claims 1 to 13, wherein the memory is in a SIM card of the device, a micro-SD of the device or a cache of the device.

15. A method as claimed in any one of claims 1 to 14, including providing a secure element partition loader, secure element partition manager, and a secure element partition cryptographic module in the NFC enabled device for implementing the method.

16. An NFC enabled device provided with secure element partitions created according to the method of any one of claims 1 to 15.

17. An NFC enabled device, comprising:

a secure element comprising a plurality of secure element partitions;

a secure element partition loader for updating or loading executable code and data into each of the secure element partitions; and

a secure element partition manager for identifying and selecting one of the secure element partitions allocated to a specific card issuer;

wherein each of the secure element partitions has a security domain comprising an access rule application master having access rules and cryptographic keys; and

the NFC enabled device further comprises a secure element partition cryptographic module for controlling access to the respective security domains of the secure element partitions.

18. A computer program product that, when executed on a computer:

creates in at least one secure element of the NFC enables device a plurality of secure element partitions; and

allocates said secure element partitions of the secure element to the respective card issuers.

19. A computer program product as claimed in claim 18, wherein when executed on a computer the computer program product also creates or locates in a memory of the NFC enabled device the at least one secure element.

20. A computer program product as claimed in either claim 18 or 19, wherein when executed on a computer the computer program product also creates in at least one of the secure element partitions a plurality of security domains for storing respective software applications or data or both software applications and data.

21. A computer readable storage medium with a computer program product according to any one of claims 18 or 20.

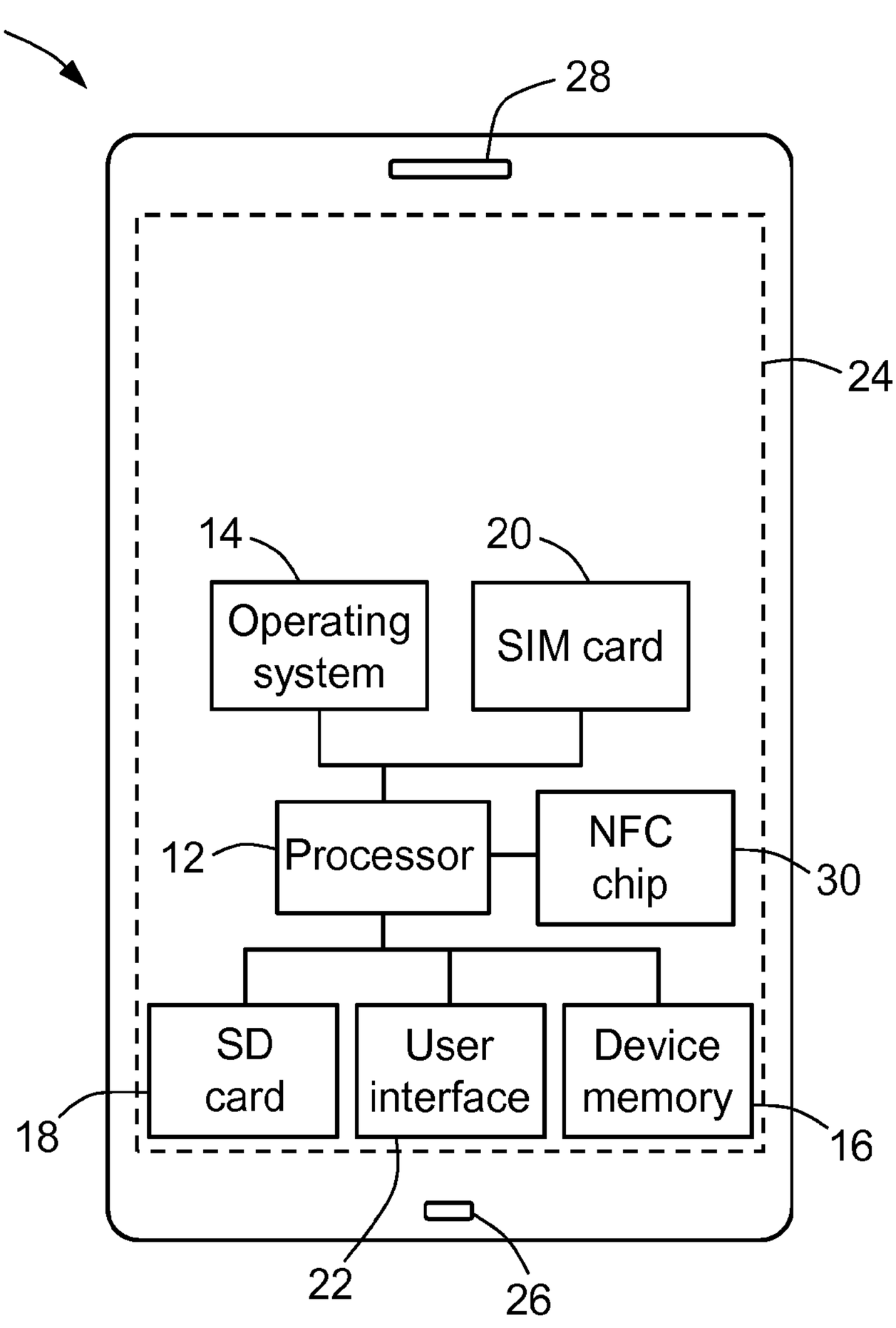

10
28
24
14
Operating system
20
SIM card
12
Processor
NFC chip
30
SD card
User interface
Device memory
18
16
22
26

Figure 1

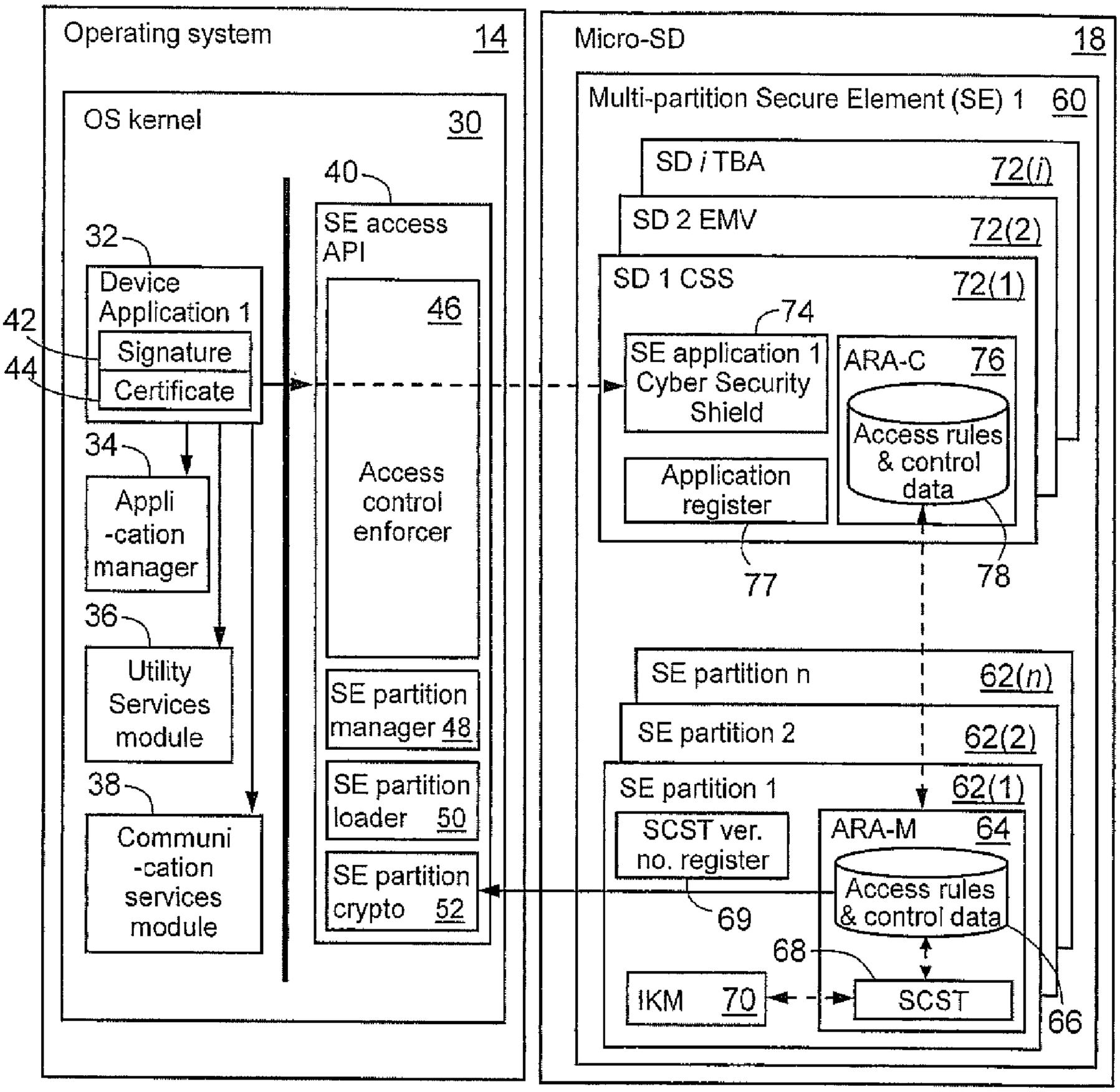

Operating system
14
OS kernel
30
40
SE access API
46
32
Device Application 1
42
Signature
44
Certificate
34
Appli -cation manager
36
Utility Services module
38
Communi -cation services module
Access control enforcer
SE partition manager 48
SE partition loader 50
SE partition crypto 52
Micro-SD
18
Multi-partition Secure Element (SE) 1
60
SD i TBA
72(i)
SD 2 EMV
72(2)
SD 1 CSS
72(1)
74
SE application 1 Cyber Security Shield
Application register
ARA-C
76
Access rules & control data
77
78
SE partition n
62(n)
SE partition 2
62(2)
SE partition 1
62(1)
SCST ver. no. register
69
ARA-M
64
Access rules & control data
68
IKM
70
SCST
66

Figure 2

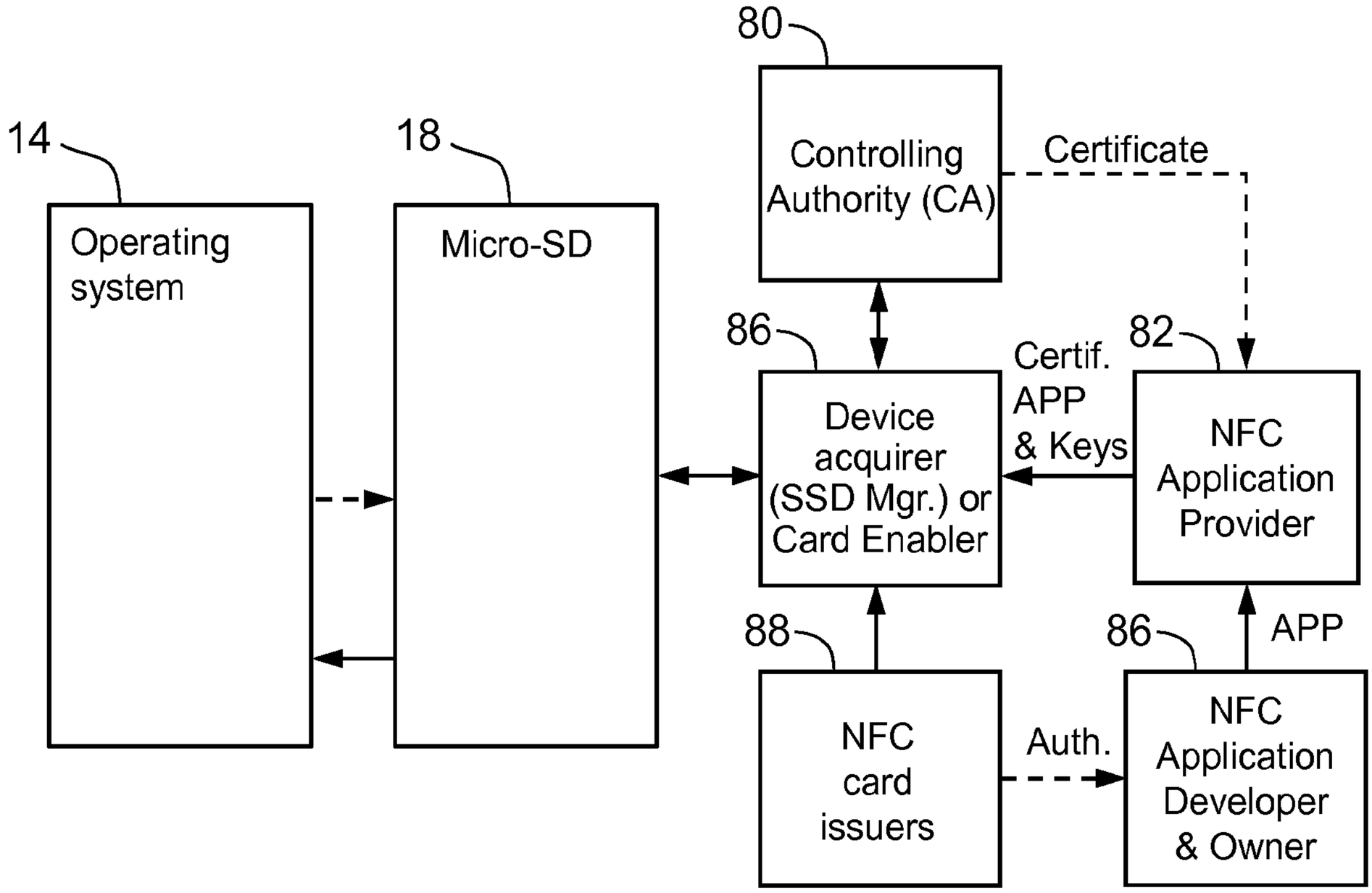

80
14
18
Operating system
Micro-SD
Controlling Authority (CA)
Certificate
86
82
Certif. APP & Keys
Device acquirer (SSD Mgr.) or Card Enabler
NFC Application Provider
88
86
APP
NFC card issuers
Auth.
NFC Application Developer & Owner

Figure 3

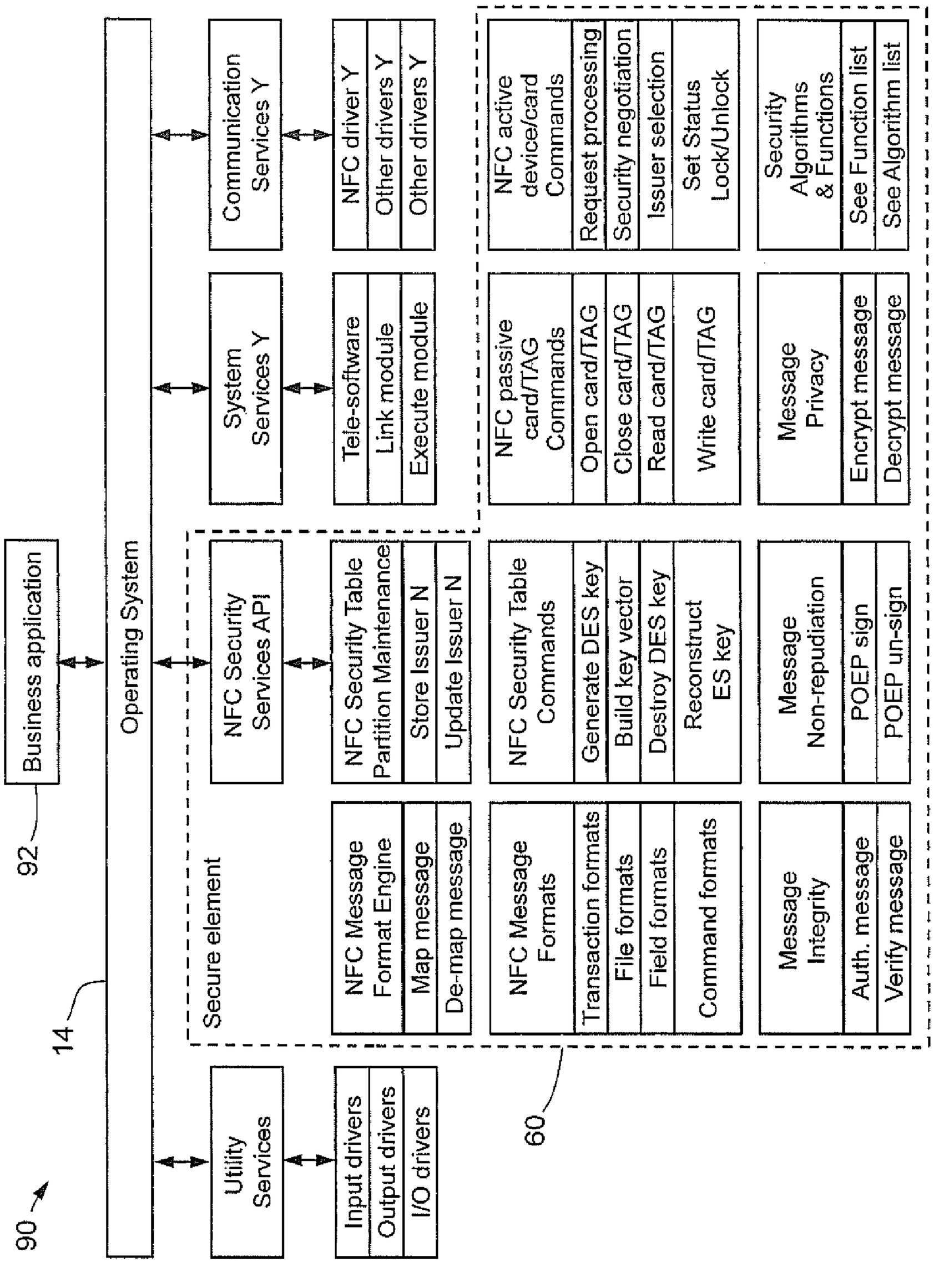

Business application
92
Operating System
14
Secure element
90
60
Communication Services Y
NFC driver Y
Other drivers Y
Other drivers Y
System Services Y
Tele-software
Link module
Execute module
NFC Security Services API
NFC Security Table Partition Maintenance
Store Issuer N
Update Issuer N
Utility Services
Input drivers
Output drivers
I/O drivers
NFC active device/card Commands
Request processing
Security negotiation
Issuer selection
Set Status Lock/Unlock
NFC passive card/TAG Commands
Open card/TAG
Close card/TAG
Read card/TAG
Write card/TAG
NFC Security Table Commands
Generate DES key
Build key vector
Destroy DES key
Reconstruct ES key
NFC Message Format Engine
Map message
De-map message
NFC Message Formats
Transaction formats
File formats
Field formats
Command formats
Security Algorithms & Functions
See Function list
See Algorithm list
Message Privacy
Encrypt message
Decrypt message
Message Non-repudiation
POEP sign
POEP un-sign
Message Integrity
Auth. message
Verify message

Figure 4

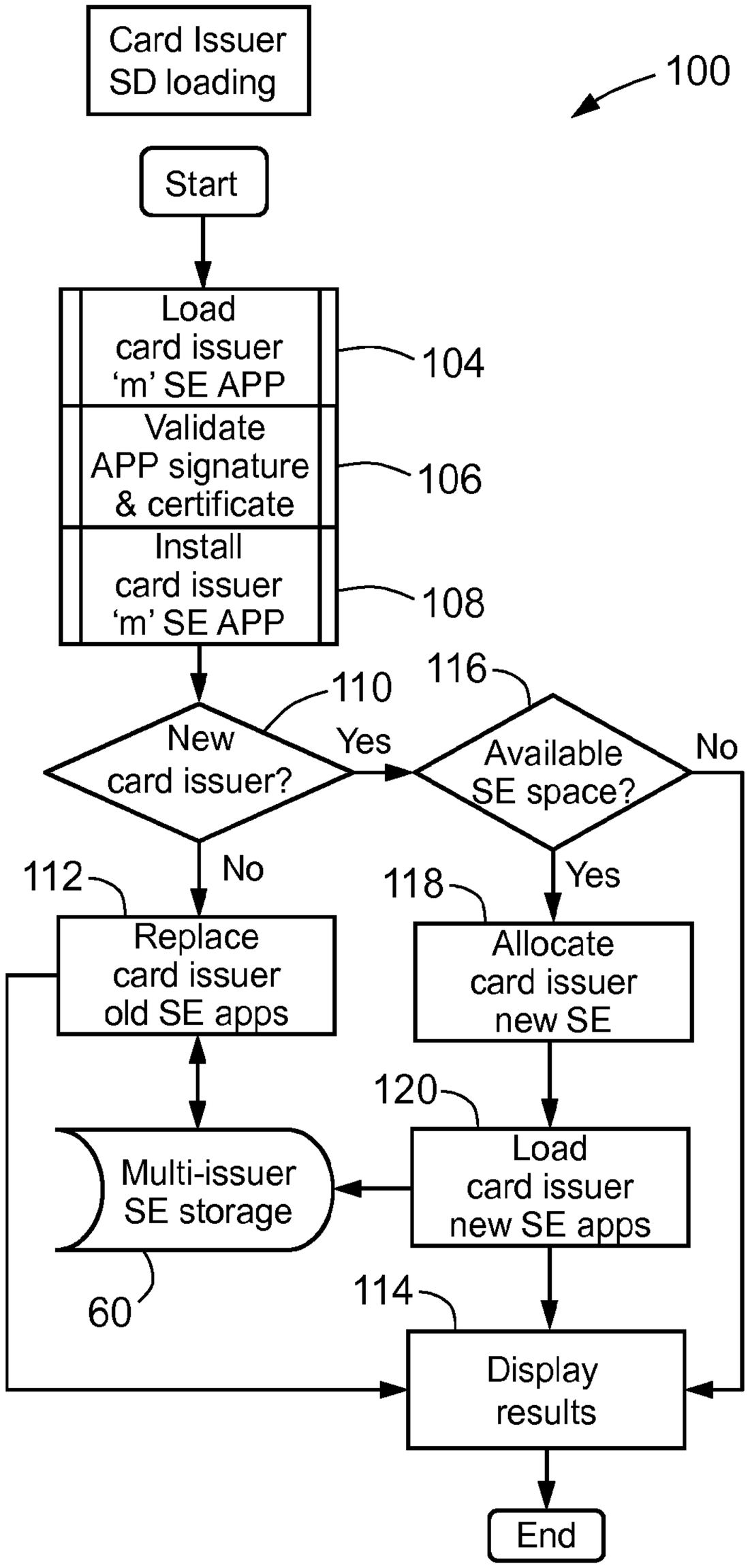

Card Issuer
SD loading
100
Start
Load
card issuer
'm' SE APP
104
Validate
APP signature
& certificate
106
Install
card issuer
'm' SE APP
108
110
New
card issuer?
Yes
116
Available
SE space?
No
112
No
Replace
card issuer
old SE apps
118
Yes
Allocate
card issuer
new SE
120
Load
card issuer
new SE apps
Multi-issuer
SE storage
60
114
Display
results
End

Figure 5A

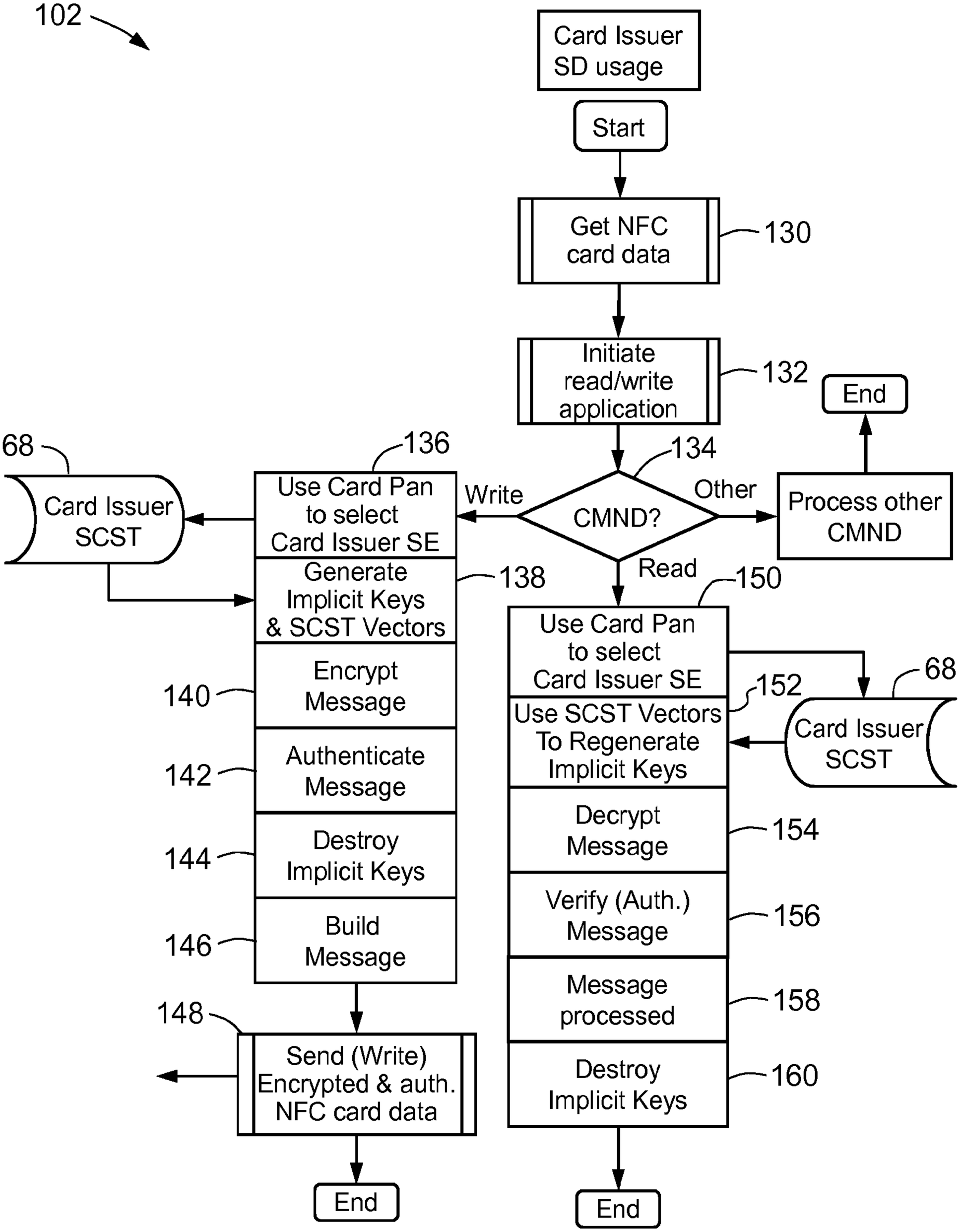

102
Card Issuer SD usage
Start
Get NFC card data
130
Initiate read/write application
132
End
68
136
134
Card Issuer SCST
Use Card Pan to select Card Issuer SE
Write
CMND?
Other
Process other CMND
Generate Implicit Keys & SCST Vectors
138
Read
150
Use Card Pan to select Card Issuer SE
68
152
Use SCST Vectors To Regenerate Implicit Keys
Card Issuer SCST
Encrypt Message
140
Authenticate Message
142
Decrypt Message
154
Destroy Implicit Keys
144
Verify (Auth.) Message
156
Build Message
146
Message processed
158
148
Destroy Implicit Keys
160
Send (Write) Encrypted & auth. NFC card data
End
End

Figure 5B

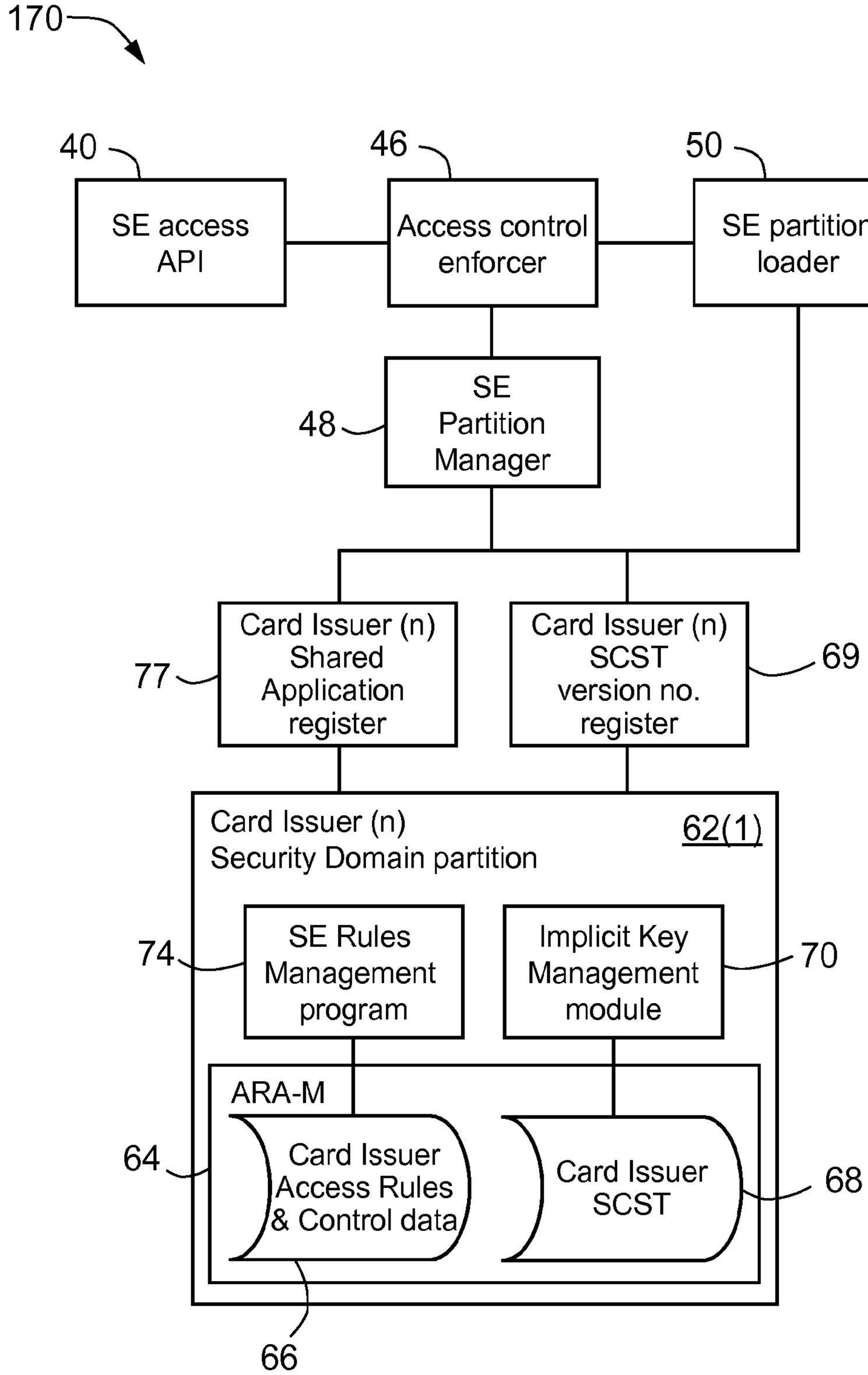
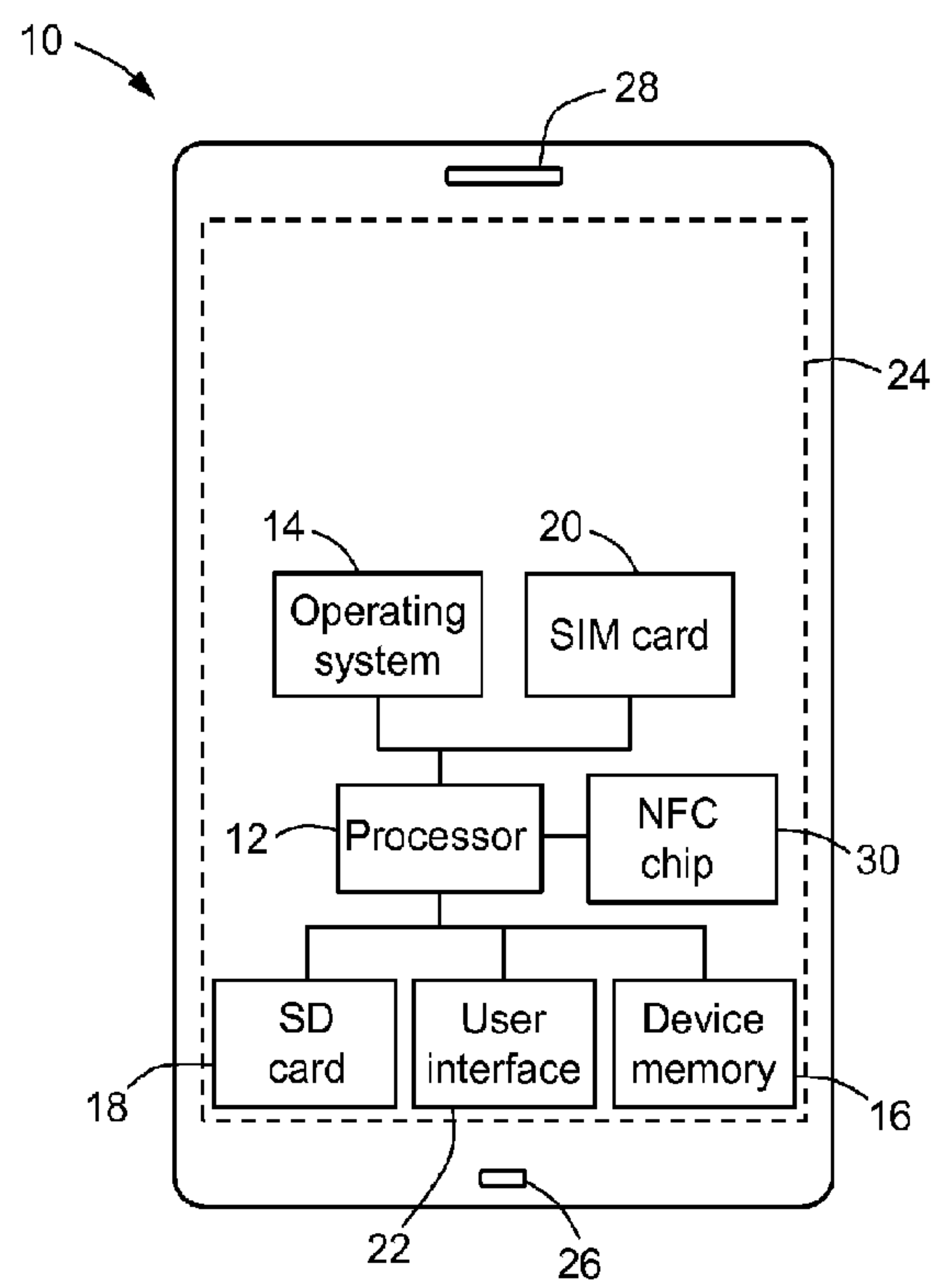

170
40
SE access API
46
Access control enforcer
50
SE partition loader
48
SE Partition Manager
77
Card Issuer (n) Shared Application register
Card Issuer (n) SCST version no. register
69
Card Issuer (n) Security Domain partition
62(1)
74
SE Rules Management program
Implicit Key Management module
70
ARA-M
64
Card Issuer Access Rules & Control data
Card Issuer SCST
68
66

Figure 6


10
28
24
14
20
Operating system
SIM card
12
Processor
NFC chip
30
SD card
User interface
Device memory
18
16
22
26