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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 December 2009 (10.12.2009)

PCT

(10) International Publication Number
WO 2009/147548 A2

(51) International Patent Classification:
G06F 21/02 (2006.01)

(21) International Application Number:
PCT/IB2009/052005

(22) International Filing Date:
14 May 2009 (14.05.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
08290481.4 27 May 2008 (27.05.2008) EP

(71) Applicant *(for all designated States except US)*: **NXP B.V.** [NL/NL]; High Tech Campus 60, NL-Eindhoven 5656 Ag (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **CORDA, Alexandre** [FR/FR]; c/o NXP Semiconductors Austria GmbH, Intellectual Property Department, Gutheil-Schoder-Gasse 8-12, A-1102 Vienna (AT).

(74) Agent: **ROEGGLA, Harald**; c/o NXP Semiconductors Austria GmbH, Intellectual Property Department, Gutheil-Schoder-Gasse 8-12, A-1102 Vienna (AT).

(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, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR),

[Continued on next page]

(54) Title: METHOD FOR STORING NFC APPLICATIONS IN A SECURE MEMORY DEVICE

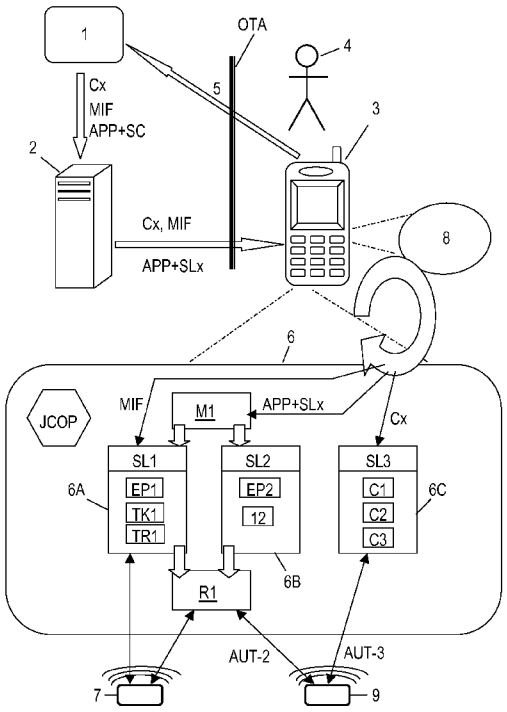

Fig. 4

(57) Abstract: A method for storing NFC applications (APP) in a secure memory device (6) having its own computational power, such as a smart card, preferably a SmartMX card, which secure memory device (6) comprises a first memory portion (6A) configured as an emulated MIFARE memory, offering a first security level (SL1), and a second memory portion (6B) accessible by means of authentication and optionally being encrypted, which second memory portion (6B) offers a second security level (SL2) which is higher than the first security level (SL1), wherein the method comprises analyzing whether the first or the second security level (SL1, SL2) is assigned to the NFC application (APP) and, depending on the results of this analysis, storing the NFC application (APP) either in the first memory portion (6A) by applying data write steps in compliance with the MIFARE standard or in the second memory portion (6B) by handling authentication routines necessary for gaining write access to said second memory portion (6B) and carrying out the write operation.

WO 2009/147548 A2

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

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

Method for storing NFC applications in a secure memory device

FIELD OF THE INVENTION

The invention relates to a method for storing NFC applications in a secure memory device.

The invention further relates to a computer program product directly loadable into the memory of a secure memory device having its own computational power.

The invention further relates to a secure memory device with an arithmetic-logic unit and a memory.

The invention further relates to a mobile communication device, preferably an NFC mobile phone.

BACKGROUND OF THE INVENTION

The MIFARE® classic family, developed by NXP Semiconductors is the pioneer and front runner in contactless smart card ICs operating in the 13.56 MHz frequency range with read/write capability. MIFARE® is a trademark of NXP Semiconductors. MIFARE complies with ISO14443 A, which is used in more than 80% of all contactless smart cards today. The technology is embodied in both cards and card reader devices. MIFARE cards are being used in an increasingly broad range of applications (including transport ticketing, access control, e-payment, road tolling, and loyalty applications). MIFARE Standard (or Classic) cards employ a proprietary high-level protocol with a proprietary security protocol for authentication and ciphering. MIFARE® technology has become a standard for memory devices with key-protected memory sectors. One example for a published product specification of MIFARE® technology is the data sheet "MIFARE® Standard Card IC MF1 IC S50 - Functional Specification" (1998) which is herein incorporated by reference. MIFARE® technology is also discussed in: Klaus Finkenzeller, "RFID Handbuch", HANSER, 4th edition (2006).

The MIFARE Classic cards are fundamentally just memory storage devices, where the memory is divided into sectors and blocks with simple security mechanisms for access control. Each device has a unique serial number. Anticollision is provided so that several cards in the field may be selected and operated in sequence.

The MIFARE Standard 1k offers about 768 bytes of data storage, split into 16 sectors with 4 blocks of 16 bytes each (one block consists of 16 bytes); each sector is protected by two different keys, called A and B. They can be programmed for operations like reading, writing, increasing value blocks, etc.. The last block of each sector is called "trailer", which contains two secret keys (A and B) and programmable access conditions for each block in this sector. In order to support multi-application with key hierarchy, an individual set of two keys (A and B) per sector (per application) is provided.

The memory organization of a MIFARE Standard 1k card is shown in Fig. 1. The 1024 X 8 bit EEPROM memory is organized in 16 sectors with 4 blocks of 16 bytes each. The first data block (block 0) of the first sector (sector 0) is the manufacturer block which is shown in detail in Fig. 2. It contains the serial number of the MIFARE card that has a length of four bytes (bytes 0 to 3), a check byte (byte 4) and eleven bytes of IC manufacturer data (bytes 5 to 15). The serial number is sometimes called MIFARE User IDentification (MUID) and is a unique number. Due to security and system requirements the manufacturer block is write protected after having been programmed by the IC manufacturer at production. However, the MIFARE specification allows to change the serial number during operation of the MIFARE card, which is particularly useful for MIFARE emulation cards like SmartMX cards.

SmartMX (Memory eXtension) is a family of smart cards that have been designed by NXP Semiconductors for high-security smart card applications requiring highly reliable solutions, with or without multiple interface options. Key applications are e-government, banking / finance, mobile communications and advanced public transportation.

The ability to run the MIFARE protocol concurrently with other contactless transmission protocols implemented by the User Operating System enables the combination of new services and existing applications based on MIFARE (e.g. ticketing) on a single Dual Interface controller based smart card. SmartMX cards are able to emulate MIFARE Classic devices and thereby makes this interface compatible with any installed MIFARE Classic infrastructure. The contactless interface can be used to communicate via any protocol, particularly the MIFARE protocol and self defined contactless transmission protocols. SmartMX enables the easy implementation of state-of-the-art operating systems and open platform solutions including JCOP (the Java Card Operating System) and offers an optimized feature set together with the highest levels of security. JCOP is an IBM® implementation of the Java Card 2.2.1 and Global Platform 2.1.1 basic specifications. JCOP handles different applications which are called applets, e.g. credit card applications. JCOP provides

authentication and encryption mechanisms. SmartMX incorporates a range of security features to counter measure side channel attacks like DPA, SPA etc.. A true anticollision method (acc. ISO/IEC 14443-3), enables multiple cards to be handled simultaneously.

It should be noted that the emulation of MIFARE Classic cards is not only restricted to SmartMX cards, but there may also exist other present or future smartcards being able to emulate MIFARE Classic cards.

Recently, mobile communication devices have been developed which contain smart cards like SmartMX cards. These mobile communication devices comprise e.g. mobile phones with Near Field Communication (NFC) capabilities, but are not limited to mobile phones.

In February 2007 the GSM Assocation (GSMA) published a white paper outlining operator community guidance for the eco-system parties involved in the development of Mobile NFC (Near Field Communication) services. Mobile NFC is defined as the combination of contactless services with mobile telephony, based on NFC technology. The mobile phone with a hardware-based secure identity token (the UICC) can provide the ideal environment for NFC applications. The UICC can replace the physical card thus optimising costs for the Service Provider, and offering users a more convenient service. Various different entities are involved in the Mobile NFC ecosystem. These are defined below:

- **Customer** – uses the mobile device for mobile communications and Mobile NFC services. The customer subscribes to an MNO and uses Mobile NFC services.
- **Mobile Network Operator (MNO)** – provides the full range mobile services to the Customer, particularly provides UICC and NFC terminals plus Over The Air (OTA) transport services.
- **Service Provider (SP)** – provides contactless services to the Customer (SPs are e.g. banks, public transport companies, loyalty programs owners etc.).
- **Trusted Service Manager (TSM)** – securely distributes and manages the Service Providers' services to the MNO customer base.

It should be mentioned that the Trusted Service Manager provides a single point of contact for the Service Providers to access their customer base through the MNOs and manage the secure download and life-cycle management of the Mobile NFC application on

behalf of the Service Providers. Depending on the national market needs and situations, the TSM can be managed by one MNO, a consortium of MNOs, or by independent Trusted Third Parties. The number of operating TSMs in one market will depend on the national market needs and circumstances.

NFC mobile phones equipped with smart cards such as SmartMX cards that comprise JCOP functionality and emulated MIFARE functionality are more and more used for ticketing, access controls, coupons, payment cards and so on. The main focus of these NFC mobile phones is the Over the Air (OTA) service provisioning of the above mentioned applications. Said applications are issued by service providers. When a service provider wants to install a new service (ticketing, access control and so on), he has two options:

- He uses the MIFARE part of the smart card which is an easy-to-access technology, but provides only a basic level of security.
- He uses the JCOP part which offers a high level of security but requires a high level of special knowledge to deal with.

Hence, there is still a need to provide easier yet very secure access to smart cards like SmartMX cards relieving the service provider from requiring special skills and knowledge about JCOP to use the very secure JCOP part of the smart cards.

OBJECT AND SUMMARY OF THE INVENTION

It is an object of the invention to provide a method of the type defined in the opening paragraph and a device of the type defined in the second paragraph, in which the disadvantages defined above are avoided.

In order to achieve the object defined above, with a method according to the invention characteristic features are provided so that a method according to the invention can be characterized in the way defined below, that is:

A method for storing NFC applications in a secure memory device having its own computational power, such as a smart card, preferably a SmartMX card, which secure memory device comprises a first memory portion configured as an emulated MIFARE memory, offering a first security level, and a second memory portion accessible by means of authentication and optionally being encrypted, which second memory portion offers a second security level which is higher than the first security level, wherein the method comprises analyzing whether the first or the second security level is assigned to the NFC application and, depending on the results of this analysis, storing the NFC application either in the first memory portion by applying data write steps in compliance with the MIFARE standard or in

the second memory portion by handling authentication routines necessary for gaining write access to said second memory portion and carrying out the write operation.

In order to achieve the object defined above, with a computer program product according to the invention characteristic features are provided so that a computer program product according to the invention is directly loadable into the memory of a secure memory device having its own computational power, comprising software code portions for performing the steps of a method according to the invention, when said product is run on the secure memory device.

In order to achieve the object defined above, a secure memory device according to the invention comprises an arithmetic-logic unit and a memory and processes the computer program product according to the above paragraph.

In order to achieve the object defined above a mobile communication device, preferably an NFC mobile phone is provided being equipped with a secure memory device according to the above paragraph.

The characteristic features according to the invention provide the advantage that a user who wants to make use of the various different security levels provided in the secure memory device does not need to have specific knowledge of how to gain access to the different memory portions. This is particularly important when the secure memory device is operated under a highly sophisticated operating system like JCOP.

The aspects defined above and further aspects of the invention are apparent from the exemplary embodiment to be described hereinafter and are explained with reference to this exemplary embodiment.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described in more detail hereinafter with reference to an exemplary embodiment. However, the invention is not limited to this exemplary embodiment.

Fig. 1 shows the memory organization of a MIFARE Standard 1k EEPROM.

Fig. 2 shows the manufacturer block of a MIFARE memory.

Fig. 3 shows the sector trailer of a sector of MIFARE memory.

Fig. 4 shows a schematic diagram of a telecommunication system including a mobile communication device with a smart card configured as a SmartMX card.

DESCRIPTION OF EMBODIMENTS

Fig. 4 shows a schematic diagram of a telecommunication system in accordance with the above referenced white book of the GSM Association (GSMA) about an eco-system for Mobile NFC (Near Field Communication) services. The telecommunication system comprises a service provider 1, a trusted service manager 2 and a mobile communication device 3. It should be observed that the numbers of service providers 1, trusted service managers 2 and mobile communication devices 3 are in no way limited. A user 4 of the mobile communication device 3 can electronically communicate (arrow 5) with the service provider 1 either by means of his mobile communication device 3 via the Over-the-Air (OTA) services provided by a mobile network operator, particularly via Short Message Service (SMS) services, and/or via a computer network. Communication between the user 4 and the service provider 1 comprises for instance ordering of NFC services like tickets etc.

The trusted service manager 2 communicates with the mobile communication device 3 via an Over-The-Air service of a mobile network operator, e.g. Short Message Service.

The service provider 1 communicates with the trusted service manager 2 via a computer network, such as the Internet, wherein the preferred data transmission protocol is HTTPS.

The mobile communication device 3 may e.g. be configured as a NFC mobile phone. The mobile communication device 3 comprises a processor (not shown in the drawing) for executing software being internally stored in the mobile communication device 3. The software comprises an operating system for carrying out and managing all functions of the mobile communication device 3.

The mobile communication device 3 is equipped with a secure memory device 6 with enhanced security features that comprises its own computational power and has multiple interface options. The secure memory device 6 is configured as a SmartMX smart card which comprises encryption coprocessors and a Java operating systems, particularly JCOP. The secure memory device 6 will be explained in more detail below. The mobile communication device 3 further comprises a trusted service client 8 which in the present embodiment of the invention is a software module being contained in the general software of the mobile communication device 3. The trusted service client 8 is controlled by the trusted service manager 2 and has the ability to manage NFC applications in the secure memory device 6. Managing NFC applications comprises installing, updating and de-installing NFC

applications. NFC applications are for instance tickets, coupons, access controls, e-purse functions, etc. which have to be handled with different levels of security.

According to the present invention, the secure memory device 6 provides different security levels for storing said NFC applications. Strictly speaking, the secure memory device 6 comprises a first memory portion 6A offering a first security level SL1. The secure memory device 6 further comprises a second memory portion 6B offering a second security level SL2 which is higher than the first security level SL1. Finally, the secure memory device 6 comprises a third memory portion 6C offering a third security level SL3 which is the highest one.

The first memory portion 6A of the secure memory device 6 is configured as an emulated MIFARE device. Access to its contents is granted by keys as has been explained in the introduction of this document. Data are written into the first memory portion 6A and read out from it according to the general MIFARE specifications. There is neither encryption nor authentication provided, but the advantage of this standard MIFARE configuration is that its access procedures can easily be handled. This first memory portion 6A is particularly useful for storing NFC applications that do not represent very high monetary values, such as a ticket TK1, a transport pass TR1, or an e-purse EP1 that represents a monetary value of less than e.g. 100 €. MIFARE applications MIF are e.g. issued by the service provider 1 and are transmitted to the trusted service manager 2. The trusted service manager 2 transmits the MIFARE application MIF via the over the air Interface (OTA) of a mobile network operator to the trusted service client 8 in the mobile communication device 3. The trusted service client 8 manages installation of the MIFARE applications MIF in the first memory portion 6A of the secure memory device 6.The contents of the first memory portion 6A of the secure memory device 6 can be read by standard MIFARE readers 7.

The configuration of the third memory portion 6C of the secure memory device 6 is based on a Java operating system, particularly JCOP, and offers highest security by providing authentication, symmetric and asymmetric encryption features. However, these features can only be used by means of so-called CARDlets which are specifically customer-tailored software modules and are based on the JCOP operating system. Consequently, any party intending to make use of these features must have an in depth knowledge of both JCOP and CARDlet programming. For instance, if a service provider 1, e.g. a ticket provider, wants to send a ticket to be stored in the third memory portion 6C of the secure memory device 6, he cannot simply transfer the ticket itself to the secure memory device 6, but he has to send a specific CARDlet C1 with its own ticket management inside in order to cope with the

specific security features of the third memory portion 6C. The service provider 1 himself has to develop this specific CARDlet C1. Due to the complexity of CARDlet programming, the third memory portion 6C is mainly used by credit card providers who have the manpower and resources for developing their customer-tailored credit card application CARDlets C2, C3. Generally, customer tailored CARDlets Cx are sent from an issuing service provider 1 to the trusted service manager 2. The trusted service manager 2 transmits the customer tailored CARDlets Cx via the over the air interface (OTA) of a mobile network operator to the trusted service client 8 in the mobile communication device 3. The trusted service client 8 installs the CARDlets Cx in the third memory portion 6C of the secure memory device 6. It should be noticed, that the described configuration of the third memory portion 6C is already state of the art and there are readers 9 existing being adapted to read the contents of the third memory portion 6C of the secure memory device 6. The readers 9 have to be programmed for carrying out authentication handling procedures AUT-3.

According to the present invention, the configuration of the second memory portion 6B of the secure memory device 6 is such that it also offers highest security by providing authentication, symmetric and asymmetric encryption features. These features are also based on a Java operating system, particularly JCOP. However, in contrast to the configuration of the third memory portion 6C, a user gets access to all these security features without the necessity for having specific knowledge about JCOP and CARDlet programming. Rather, according to the present invention there is a specific management CARDlet M1 provided in the secure memory device 6 that manages all installation routines and deals with the particulars of high-level security. This means that according to the present invention a service provider 1 who wants to send an NFC application APP to the secure memory device 6 only has to send this application APP together with a security criterion SC to the trusted service manager 2. It should be emphasized, that beyond knowing the security criterion SC the service provider 1 does not have to have knowledge of how to deal with the high-level security features like authentication, symmetric and asymmetric encryption, and particularly does not need to know anything about JCOP and CARDlet programming.

The security criterion SC is e.g. either a code for the desired security level SL1, SL2, SL3, or a specific value that can be checked by the trusted service manager 2 in respect of predefined conditions. For instance, the trusted service manager 2 checks incoming e-purse applications whether they have a monetary value of e.g. less than 100 €. If this condition is met, then the trusted service manager 2 will e.g. assign the security level SL1 to

this e-purse application, otherwise he will assign the higher security level SL2 to this e-purse application.

Next, the trusted service manager 2 transmits the NFC application APP together with the assigned security level SLx (x = 1 or 2) via the over the air interface OTA of a mobile network operator to the trusted service client 8 residing in the mobile communication device 3. The trusted service client 8 hands the NFC application APP together with the assigned security level SLx over to the specific management CARDlet M1 in the secure memory device 6. The specific management CARDlet M1 analyses which security level SLx is assigned to the NFC application APP.

If the first security level SL1 is assigned to the NFC application APP then the specific management CARDlet M1 will store the NFC application APP in the first memory portion 6A in accordance with the standard MIFARE specifications.

If the second security level SL2 is assigned to the NFC application APP then the specific management CARDlet M1 will handle all necessary encryption and/or authentication steps in order to get write access to the second memory portion 6B of the secure memory device 6 and will store the NFC application APP in the second memory portion 6B. It should be mentioned that the specific management CARDlet M1 has implemented all necessary information and procedures for handling encryption and/or authentication in respect of the second memory portion 6B, but has no information to access the third memory portion 6C of the secure memory device 6.

In order to enable MIFARE reader 7 or reader 9 which is adapted for carrying out authentication AUT-2, a specific reading CARDlet R1 is provided which has read access to both the first memory portion 6A and the second memory portion 6B, such that it retrieves MIFARE applications from the first memory portion 6A and transmits them to the MIFARE reader 7 and - provided that authentication with reader 9 was successful - retrieves NFC applications from the second memory portion 6B and transmits them to the reader 9.

It should be noted that the above-mentioned embodiments illustrate rather than limit the invention, and that those skilled in the art will be able to design many alternative embodiments without departing from the scope of the appended claims. In the claims, any reference signs placed between parentheses shall not be construed as limiting the claim. The word "comprising" does not exclude the presence of elements or steps other than those listed in a claim. The indefinite article "a" or "an" preceding an element does not exclude the presence of a plurality of such elements. In the device claim enumerating several means, several of these means may be embodied by one and the same item of hardware. The mere

fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.

CLAIMS:

1. A method for storing NFC applications (APP) in a secure memory device (6) having its own computational power, such as a smart card, preferably a SmartMX card, which secure memory device (6) comprises a first memory portion (6A) configured as an emulated MIFARE memory, offering a first security level (SL1), and a second memory portion (6B) accessible by means of authentication and optionally being encrypted, which second memory portion (6B) offers a second security level (SL2) which is higher than the first security level (SL1), wherein the method comprises analyzing whether the first or the second security level (SL1, SL2) is assigned to the NFC application (APP) and, depending on the results of this analysis, storing the NFC application (APP) either in the first memory portion (6A) by applying data write steps in compliance with the MIFARE standard or in the second memory portion (6B) by handling authentication routines necessary for gaining write access to said second memory portion (6B) and carrying out the write operation.

2. The method as claimed in claim 1, wherein the secure memory device (6) is operated by means of a Java operating system, preferably JCOP.

3. A computer program product being directly loadable into the memory of a secure memory device (6) having its own computational power, comprising software code portions for performing the steps of a method according to claim 1 or 2, when said product is run on the secure memory device (6).

4. A computer program product as claimed in claim 3, wherein the computer program product is stored on a computer readable medium or is downloadable via a data connection from a remote server.

5. A computer program product as claimed in claim 3, being designed to run under a Java operating system, particularly JCOP.

6. A secure memory device (6) with an arithmetic-logic unit and a memory, wherein the secure memory device (6) is adapted to process the computer program product as claimed in claim 3.

7. The secure memory device (6) as claimed in claim 6, being configured as a smart card, preferably a SmartMX card.

8. A mobile communication device (3) comprising the secure memory device (6) as claimed in claim 7.

9. The mobile communication device (3) as claimed in claim 8, being configured as an NFC mobile phone.

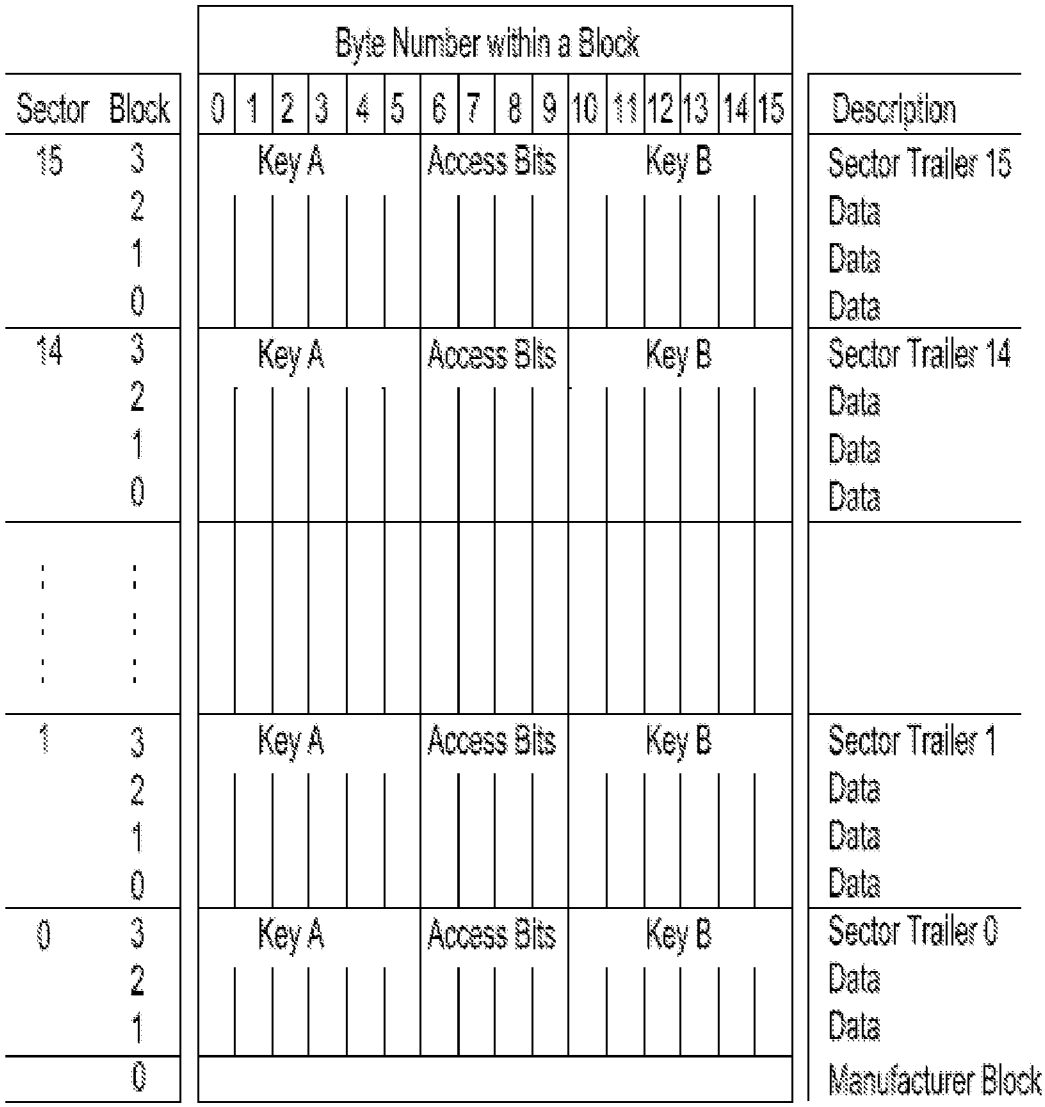

Fig. 1

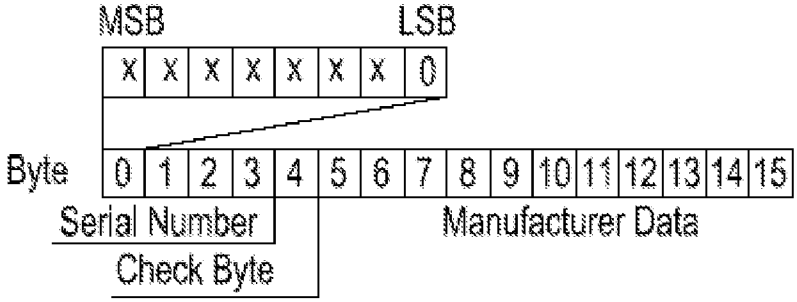

Fig. 2

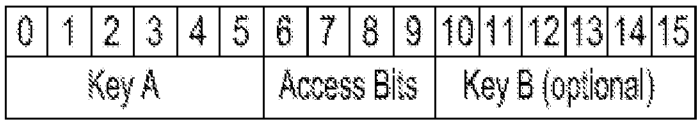

Fig. 3

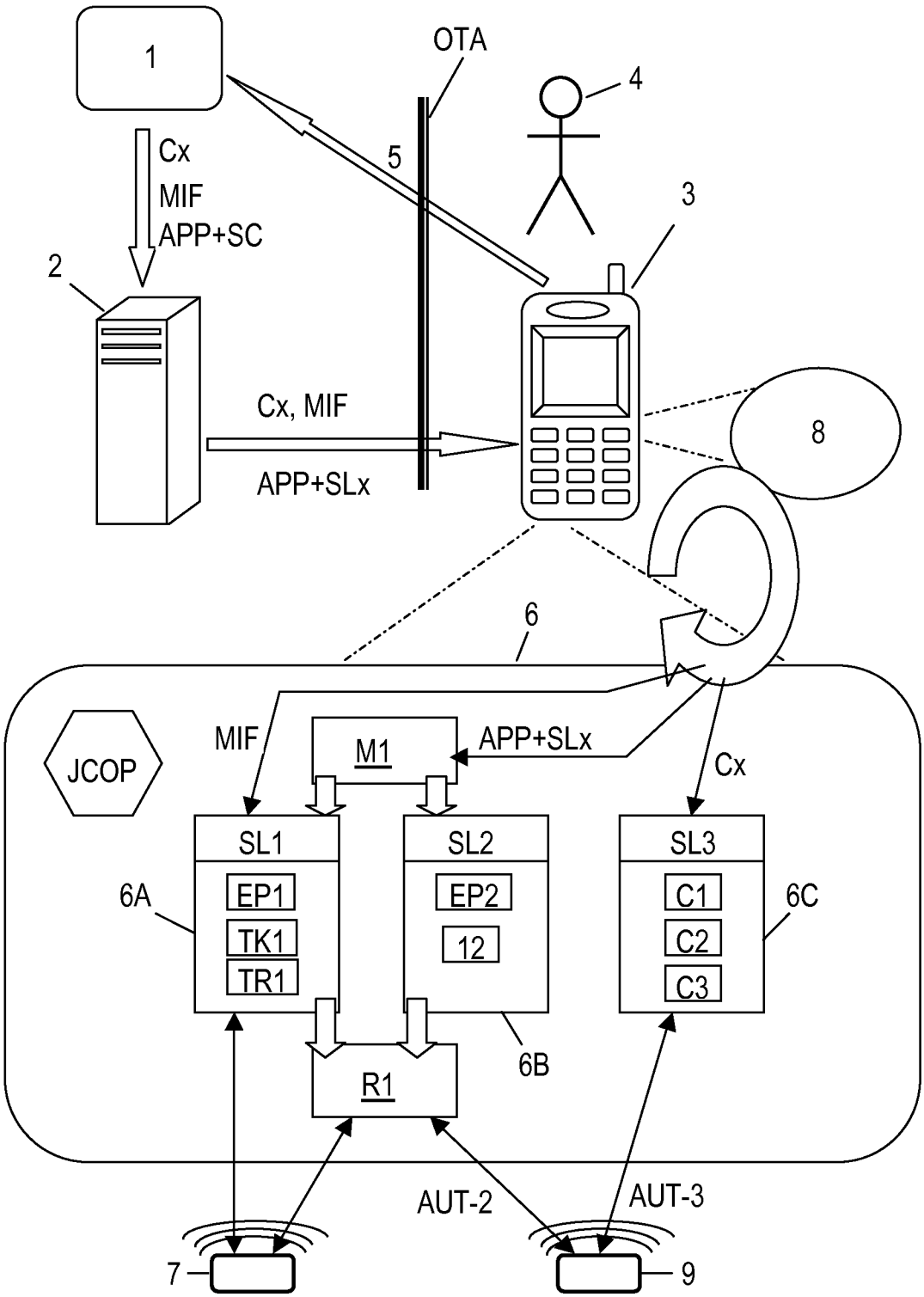
1
OTA
4
Cx
MIF
APP+SC
5
3
2
Cx, MIF
APP+SLx
8
6
JCOP
MIF
M1
APP+SLx
Cx
SL1
SL2
SL3
6A
EP1
TK1
TR1
EP2
12
C1
C2
C3
6C
6B
R1
AUT-2
AUT-3
7
9

Fig. 4