

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
10 July 2008 (10.07.2008)

PCT

(10) International Publication Number
WO 2008/081370 A2

(51) International Patent Classification:
G06F 17/30 (2006.01)

Department, Gutheil-Schoder-Gasse 8-12, A-1102 Vienna (AT).

(21) International Application Number:
PCT/IB2007/055027

(74) Agents: **RÖGGLA, Harald** et al.; NXP Semiconductors Austria GmbH, Intellectual Property Department, Gutheil-Schoder-Gasse 8-12, A-1102 Vienna (AT).

(22) International Filing Date:
11 December 2007 (11.12.2007)

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, 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, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
06026940.4 27 December 2006 (27.12.2006) EP

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

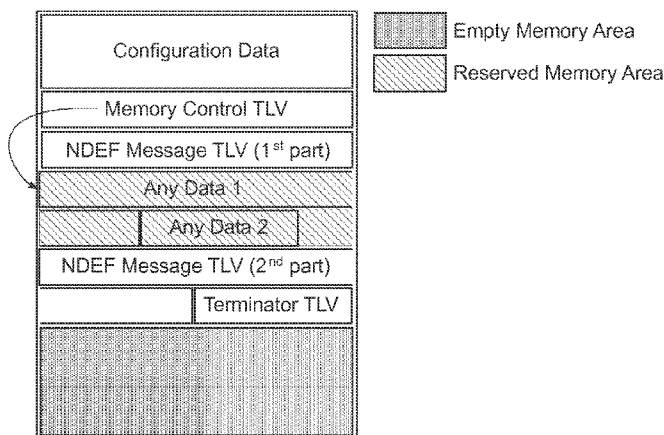
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **GALLO, Francesco** [IT/DE]; c/o NXP Semiconductors Austria GmbH, Intellectual Property Department, Gutheil-Schoder-Gasse 8-12, A-1102 Vienna (AT). **MEYN, Hauke** [DE/DE]; c/o NXP Semiconductors Austria GmbH, Intellectual Property

[Continued on next page]

(54) Title: A METHOD FOR STORING DATA AS WELL AS A TRANSPONDER, A READ/WRITE-DEVICE, A COMPUTER READABLE MEDIUM INCLUDING A PROGRAM ELEMENT AND SUCH A PROGRAM ELEMENT ADAPTED TO PERFORM THIS METHOD



(57) Abstract: A method for storing or reading data in a memory array of a transponder and a corresponding transponder, read/write device and program element is described. Therein, a data structure for storing data within the memory array is defined by a predetermined protocol. The data structure comprises: a header data block including predefined header data; an application data block for storing application data; a memory control data block including a reservation indicator for indicating a reserved partial memory area of the memory array where, in accordance with the predetermined protocol, application data cannot be read or written by a protocol compliant reader device. The method for storing data comprises storing additional application data in the reserved partial memory area. Thereby, memory areas which, according to the predetermined protocol, are not used can be used for new applications, data can be hidden in these areas such that they can not be read by protocol compliant reader devices and the data structure read or written by the method of the invention is compatible with the former predetermined protocol.

WO 2008/081370 A2



Declaration under Rule 4.17:

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

Published:

— *without international search report and to be republished upon receipt of that report*

A method for storing data as well as a transponder, a read/write-device, a computer readable medium including a program element and such a program element adapted to perform this method

5

Field of invention

The present invention relates to the field of storing and reading data in a transponder wherein data can be stored in accordance with a storage protocol. Particularly, the present invention relates to storing and reading additional data in a transponder such as an all contactless memory card or a RFID (Radio Frequency IDentification) tag in which data can be stored in accordance with the Type 2 Tag Operation standardization of the NFC Forum.

15

Art Background

Identification products such as smart cards and RFID tags are used widely in fields such as transport (ticketing, road tolling, baggage tagging), finance (debit and credit cards, electronic purse, merchant card), communications (SIM card for GSM phone), and tracking (access control, inventory management, asset tracking). Radio Frequency IDentification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. An RFID tag is an object that e.g. can be attached to or incorporated into a product, animal, or person e.g. for the purpose of identification using radio waves. Chip-based RFID tags contain e.g. silicon chips and antennas. Passive tags require no internal power source, whereas active tags require a power source.

25

International standard ISO14443A is an industry standard for contactless smart cards.

ISO14443A-compliant products provide RF communication technology for transmitting data between a card or tag and a reader device. For example, in electronic ticketing for public transport, travelers just wave their card over a reader at the turnstiles or entry point, benefiting from improved convenience and speed in the ticketing process. Such products are

30

set to be the key to individual mobility in the future, supporting multiple applications including road tolling, airline tickets, access control and many more.

5 Evolving from a combination of contactless identification and networking technologies, Near Field Communication (NFC) (see for example the standard ISO 18092) is a very short-range wireless technology, for distances measured in centimeters, and is optimised for intuitive, easy and secure communications between various devices without user configuration. In order to make two devices communicate, users bring them close together or even make them touch. The devices' NFC interfaces will automatically connect and configure themselves to form a peer-to-peer network. NFC can also bootstrap other protocols like Bluetooth™ or 10 Wireless Ethernet (WiFi) by exchanging the configuration and session data. NFC is compatible with contactless smart card platforms. This enables NFC devices to read information from these cards, making contactless smart cards the ideal solution for bringing information and vouchers into the NFC world.

15

NFC devices can also operate like a contactless card making them compatible with the huge installed infrastructure of ISO14443A-compliant systems. This functionality is called card emulation. Secure NFC combines NFC applications with smart card security. Devices with secure NFC act like a contactless smart card with cryptographic capabilities. This means that 20 confidential data, and data that represents values, is stored in a secure memory area and always stays on the card. Authentication is performed by the NFC device itself and transmitted data can be encrypted by the NFC device using a private encryption key stored in the device's secure memory.

25 The Near Field Communication Forum (NFC Forum) is a non-profit industry association founded by Nokia Corporation, Royal Philips Electronics and Sony Corporation to advance the use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs. The NFC Forum will promote implementation and standardization of NFC technology to ensure interoperability between devices and services.

30

To store NFC Forum defined data (called NDEF) e.g. inside contactless cards or RFID tags four different draft specifications have been made called: "Type 1 Tag Operational", "Type 2 Tag Operational", "Type 3 Tag Operational" and "Type 4 Tag Operational".

This invention is related inter alia to all contactless cards or RFID tags that are compliant to the "Type 2 Tag Operational" specification draft of the NFC Forum (available e.g. from www.nfc-forum.org). The "Type 2 Tag Operational" draft specification shows how to store data inside transponders used as NFC devices such as e.g. contactless cards and RFIDs.

5

There may be a need for an alternative way of storing and reading data in transponders such as contactless cards or RFID tags. Especially, there may be a need for a way of storing additional data in transponders such that the additional data is not accessible using a reader device which is compliant with a standardization protocol such as the "Type 2 Tag
10 Operational" draft specification and such that it does not interfere with data stored in compliance with the standardization protocol. Furthermore, there may be a need for corresponding transponder devices, read/write devices, computer program elements and computer readable media for implementing such storing/reading method.

15

Summary of the Invention

This need may be met by the subject matter according to the independent claims.

Advantageous embodiments of the present invention are described in the dependent claims.

20

According to a first aspect of the invention there is provided a method for storing data in a memory array of a transponder. Therein, a data structure for storing data within the memory array is defined by a predetermined protocol. The data structure comprises: a header data block including predefined header data; an application data block for storing application data;
25 and a memory control data block including a reservation indicator for indicating a reserved partial memory area of the memory array where, in accordance with the predetermined protocol, application data cannot be read or written by a protocol compliant reader device. According to the invention the method comprises the step of storing additional application data in the reserved partial memory area.

30

This aspect of the invention is based on the idea that transponders have a memory array of predetermined size. In this memory array, data can be stored. A structure of such stored data is predetermined by a given protocol such that data included in the data structure can be read

or written by a protocol compliant read/write device being adapted to operate in accordance with the protocol.

The protocol defines that all application data is to be stored within the application data block.

5 This application data block does not need to be continuous but can include separate data blocks having non-used, blocked or reserved memory areas in between. In accordance with the protocol, a reservation indicator indicates a reserved partial memory area within the memory array. This reservation indicator provides an indication to a read/write device operating in accordance with the predetermined protocol that application data is not allowed
10 to be read or written in the blocked or reserved memory area. In other words, when a read device which is adapted to operate in accordance with the protocol reads data from the application data block, it is forced to jump over the indicated blocked or reserved memory area. On the other side, a write device which is adapted to operate in accordance with the protocol will write data into the application data block only in areas apart from the reserved
15 memory area.

The method of the first aspect uses the data structure in accordance with the predetermined protocol but includes the additional feature that additional application data can also be stored in the memory array of the transponder in a reserved memory area which can not be accessed
20 by a protocol compliant read/write device. In other words, the reservation indicator can be read but instead of indicating that in the reserved memory area no application data is allowed to be stored it can serve as an indication that in this reserved memory area additional application data can be stored.

25 Several advantages can be achieved with the invention. Memory space as e.g. a reserved or blocked memory area which according to the protocol is not used can be used for storing additional application data. As a protocol compliant reader device would not access the reserved or blocked memory these additional data can be hidden from access of such conventional reader device. At the same time, the data conventionally stored within the
30 application data block in accordance with the protocol will not interfere with the additional application data. This provides backwards compatibility, i.e. a read/write device operating in accordance with the method of the present invention will manipulate the data structure within the memory of a tag only in a way that it remains compatible with conventional protocol compliant read/write devices.

In the following further details, definitions, features and characteristics about the method of the first aspect are given.

5 A transponder can be an active element, i.e. having a power source, or a passive element, i.e. without power source, being adapted for near field communication. For example, a transponder can be a RFID tag or a contactless card. Alternatively, the transponder can be an active device which emulates e.g. a tag. For example, the transponder can be included in a mobile phone having a battery wherein the transponder emulates the functions of an RFID
10 tag such that a user can use his mobile phone like an RFID tag. The transponder can include a circuitry establishing an array of volatile or rewritable memory of predetermined size such as for example 64 Bytes or more.

A protocol can be used as a standard or specification defining how data are to be stored in the
15 memory in terms of order and content. For example, the protocol can define which information is to be stored at a specific position within the memory array. Furthermore, the protocol can specify indicators or flags. A protocol specifically adapted for transponders is the "Type 2 Tag Operation specification" of the NFC Forum. It specifies, with a set of rules and guidelines, the operation of a NFC Forum Type 2 Tag which can be a tag, card or token
20 compatible with the NFC Forum Type 2 specification and including a contactless IC chip, which has build-in memory and memory access functions. This protocol also defines how application data defined according to the NFC Data Exchange Format (NDEF) is detected, read from, and written to the Type 2 Tag in order to achieve and maintain interchangeability and interoperability at the NFC Forum Type 2 Tag read/write level.

25 The data structure within the memory array of the transponders can include several data blocks.

The header data block can include predefined header data including e.g. a unique
30 identification code, a manufacturer code and static lock bytes representing a field-programmable read-only locking mechanism.

Application data to be stored in the application data block can include any kind of data. For example, data specific to an application to be run in the transponder or in a coupled

read/write device can be stored. Alternatively, user specific data including e.g. authentication information can be stored. If the Type 2 Tag Operation specification of the NFC Forum is used as the protocol, the application data can include the NDEF message as specified in this protocol.

5

An optional terminator data block mainly provides the information that the application data block, which does not necessarily have a predetermined size, ends at this position. Basically, it can be provided as a single byte the content of which serves as a flag.

10 The memory control data block can be located anywhere within the memory area. Preferably, it is located between the header data block and the application data block. The reservation indicator for indicating the reserved partial memory area can be the only content of the memory control data block. Alternatively, the memory control data block can contain further information defining e.g. special purposes within the predetermined protocol. The reservation
15 indicator can indicate a position or address within the memory array. From this position or address, a reserved memory area of predetermined size can extend. Alternatively, the reservation indicator can indicate a position or address and further more a size of the reserved memory area. The reservation indicator can also indicate a plurality of reserved memory areas. Alternatively, a plurality of reservation indicators can be included in the memory
20 control data block.

The additional application data to be stored in the reserved memory area in accordance with the present invention can include any kind of data. It is not limited to a specific data format. E.g. it can avoid to use the overhead required by "Type 2 Tag Operational" specification
25 draft and NFC Data Exchange Format (NDEF) as will be understood from the description further below.

According to an embodiment the method further comprises the step of storing a storage indicator for indicating that additional application data is stored within the reserved partial
30 memory area. The storage indicator can be stored anywhere within the memory array, e.g. in the header data block, the application data block, the memory control data block or the optional terminator data block. For example, the storage indicator can be stored within reserved partial memory area right behind its starting position or just before its end position.

Alternatively, the storage indicator can be stored at a predetermined position within the memory control data block.

5 The storage indicator can simply indicate that additional data is stored somewhere in an indicated reserved memory area and a reader device would have to search for the stored additional data autonomously using for example predetermined flags or a look-up table. Alternatively, the storage indicator can include information as to the position (e.g. absolute or relative to the position of a starting or end position of the reserved memory area), length, type or content of the stored additional application data. Then, the method can be performed
10 taking into account at least one of these data. This can simplify and accelerate the finding and processing of additionally stored data.

In a second aspect of the invention a method for reading data in a memory array of a transponder is provided wherein a data structure for storing data within the memory array is
15 defined by a predetermined protocol as outlined with respect to the first aspect. The method comprises: reading additional application data stored within the reserved memory area.

The second aspect is based on the idea to modify a method of reading data in accordance with the predetermined protocol such that, instead of ignoring the reserved memory area, a
20 reader device can be specifically adapted to read additional data from this reserved memory area.

In an embodiment of the second aspect, the method includes searching for a storage indicator stored within the memory array, e.g. in at least one of the header data block, the application
25 data block and the memory control data block, wherein the storage indicator includes data for indicating that additional application data is stored within the reserved memory area. The storage indicator can have the features as outlined above with respect to the first aspect.

In an embodiment in accordance with the above first or second aspect, the reservation
30 indicator included in the memory control data block causes a protocol compliant reader device to jump over the indicated reserved partial memory area when storing or reading data in the memory array. That means, a read/write device that operates in compliance with the predetermined protocol can read/write data stored within the application data block before the reserved partial memory area and, when reaching a reserved memory area, can optionally

continue reading/writing behind the reserved memory area. Accordingly, additional data stored in the reserved memory area will be hidden from the protocol compliant read/write device and can only be read/written with a read/write device operating in accordance with the above described method of the invention.

5

In a third aspect of the invention a transponder is provided in which data is stored and can be read in accordance with one of the above aspects or embodiments. The transponder can be an RFID tag or a contactless smart card or a device emulating such devices.

10

In a fourth aspect of the invention a read/write-device is provided which is adapted to perform the method according to one of the above aspects or embodiments. Specifically, the read/write-device can be able to find a memory data block and to detect a reservation indicator included therein. It can retrieve information about the position of additionally stored application data from the reservation indicator and read the additionally application data stored in the reserved memory area.

15

In a fifth aspect of the invention a computer readable medium is provided, the medium including a program element adapted to perform the method according to one of the above aspects or embodiments.

20

In a sixth aspect of the invention a program element is provided which is adapted to perform the method according to one of the above aspects or embodiments.

25

On the basis of the above given and the following explanation of the methods for storing or reading data in a transponder a skilled person will be able to translate the steps of the method into a computer program element for carrying out the method.

30

It has to be noted that embodiments of the invention are described with reference to different subject matters. In particular, some embodiments are described with reference to apparatus type claims whereas other embodiments are described with reference to method type claims. However, a person skilled in the art will gather from the above and the following description that, unless other notified, in addition to any combination of features belonging to one type of subject matter also any combination between features relating to different subject matters, in

particular between features of the apparatus type claims and features of the method type claims is considered to be disclosed with this application.

5 The aspects defined above and further aspects of the present invention are apparent from the examples of embodiment to be described hereinafter and are explained with reference to the examples of embodiments. The invention will be described in more detail hereinafter with reference to examples of embodiments but to which the invention is not limited.

10 Brief Description of the Drawings

Fig. 1 shows an example of a data structure in accordance with the Type 2 tag Operation specification of the NFC Forum.

15 Fig. 2 schematically shows an exemplary data structure which can be read or written according to a an embodiment of the present invention.

Fig. 3 schematically shows another exemplary data structure which can be read or written according to a another embodiment of the present invention.

20

Detailed description of embodiments

In the following, embodiments of the present invention are described wherein the Type 2 Tag
25 Operation specification of the NFC Forum (herein also called in the following “type 2 tag protocol”) is used as the predetermined protocol. Main features of this protocol are described herein and the terminology used in this protocol will be used in the following description. Further details concerning this protocol can be obtained from the NFC Forum’s publications available e.g. via www.nfc-forum.org. A read/write device which is adapted to operate in
30 accordance with the type 2 tag protocol will also be referred as “NFC Forum Device” herein.

The following conventions and notations apply in this document unless otherwise stated:

Binary numbers are represented by strings of digits 0 and 1 shown with the most significant bit (msb) left and the least significant bit (lsb) right , “b” is added at the end.

Example: 11110101b

Hexadecimal numbers are represented is using the numbers 0 - 9 and the characters A – F, a
5 “h” is added at the end. The Most Significant Byte (MSB) is shown on the left, the Least Significant Byte (LSB) on the right.

Example: F5h

Decimal numbers are represented as is (without any tailing character).

Example: 245

10

A type 2 tag is based on a particular memory chip with a certain memory size and space for data. The method of the present invention is especially applicable to tags of the type having a dynamic memory structure. This memory structure (or layout) is applied to Type 2 tags with a memory size bigger than 64 bytes. Fig. 1 shows an example of a memory layout of such
15 tag. It is comprises different fields:

- UID, Unique identifier
- Internal, bytes for manufacturing usage
- Reserved, reserved bytes
- Lock, static and dynamic lock bytes, to switch the tag from READ/WRITE state to
20 READ-ONLY state
- CC, Capability Container bytes
- Data, bytes used to store information

In Fig. 1 each block is numbered from 0 to k. The block n indicates the last block of the data
25 area of the memory array. Blocks from n+1 to k contain reserved or lock bytes.

Dynamic lock bytes and reserved bytes might be located at any byte address in between or at the end of the data areas starting from block 16.

It is to be noted that in the context of this application the term “reserved memory area” as used in the claims can include one or both of the reserved bytes and the lock bytes as defined in the type 2 tag protocol.

- 5 Reserved bytes belonging to reserved memory areas shall be ignored / jumped over during read and write operations with a NFC Forum device. Reserved bytes shall be identified by one or more Memory Control TLV blocks.

In the type 2 tag protocol TLV blocks are defined. A TLV block shall consist of one to three fields:

10

T (tag field, or T field) shall identify the type of the TLV block and shall consist of a single byte encoding a number from 00h to FFh.

15

L (length field, or L field) shall provide the size in bytes of the value field. It has two different formats composed of one, or three bytes. The NFC Forum Device shall understand all two length field formats.

20

V (value field, or V field) If the length field is equal to 00h or there is no length field, there shall not be the value field, i.e. the TLV block is empty. If there is the length field and indicates a length of the value field N bigger than zero (N>0), the value field shall consist of N consecutive bytes.

The following table lists the TLV blocks specified by the type 2 tag operation specification:

TLV block name	Tag Field Value	Short Description
NULL TLV	00h	It might be used for padding of memory areas and the NFC Forum Device shall ignore this
Lock Control TLV	01h	It defines details of the lock bits
Memory Control TLV	02h	It identifies reserved memory areas

NDEF Message TLV	03h	It contains an the NDEF message
Proprietary TLV	FDh	Tag proprietary information
Terminator TLV	FEh	Last TLV block in the data area

The TLV blocks shall be written in a specific order inside the data area:

- NDEF Message TLVs and Proprietary TLVs are present after all Lock Control TLVs and Memory Control TLVs.
- 5 - if present, the Terminator TLV is the last TLV block on the Type 2 tag platform

The Lock Control TLV may be present inside the Type 2 tag, and an NFC Forum Device shall be able to read/process it. It provides control information about the lock areas where the dynamic lock bytes are located . Each Lock Control TLV shall indicate a single lock area.

- 10 More lock areas shall be indicated using more Lock Control TLV blocks. Below the encoding of the 3 TLV fields of Lock Control TLV are shown:

T SHALL be equal to 01h (see Table 2).

L SHALL be equal to 03h.

- 15 V SHALL be composed of 3 bytes that uniquely identify the position and the size of the lock area, and the number of pages locked by each bit of the dynamic lock bytes. The 3 bytes SHALL be encoded in the following way:

- Position, MSB. It codes the position inside the tag of the lock area. The position byte consists of 2 parts (to calculate the bytes address from the position byte see below):
 - o PagesAddr, most significant nibble (4 bits), coded as number of pages
20 (0h=0...Fh=15) and
 - o ByteOffset, least significant nibble, coded as number of bytes (0h=0...Fh=15).
- Size, middle byte, coded as number of bits (01h=1...FFh=255, 00h=256). It indicates the size in bits of the lock area.
- Page control, LSB. The page control provides general control information: the size in
25 bytes of a page, and the number of bytes that each dynamic lock bit is able to lock. Page control byte is split up into two nibbles of 4 bits each:

o BytesPerPage: least significant nibble, coded as 2^n (0h=RFU, 1h=1...Fh=15). It indicates the number of bytes per page.

o BytesLockedPerLockBit: most significant nibble, coded as 2^n (0h=RFU, 1h=1...Fh=15). It indicates the number of bytes that each dynamic lock bit is able to lock.

From the position byte, the byte address (ByteAddr) of the lock area shall be calculated in the following way:

$$\text{ByteAddr} = \text{PageAddr} * 2^{\text{BytesPerPage}} + \text{ByteOffset}$$

The ByteAddr is calculated from the beginning of the overall memory tag; Byte 0 of Block 0 is indicated by ByteAddr equal to 0.

The byte address shall be used to read and write the relative lock area using the appropriate READ and WRITE commands. The page definition has nothing to do with the block definition used by READ and WRITE commands. The block has a fixed size equal to 4 bytes instead the size of a page is defined by the BytesPerPage field.

It is to be noted that the lock Control TLV might be skipped if a Type 2 tag is in READ-ONLY state. Lock Control TLV blocks can be replaced by Memory Control TLV indicating the same memory areas for Type 2 tag in READ-ONLY state.

The Memory Control TLV may be present inside the Type 2 tag, and an NFC Forum Device shall be able to read/process it. It provides control information about the reserved areas where the reserved bytes are located, and the size of the reserved bytes.

If the Type 2 tag is delivered by the vendors in READ-ONLY state, the Memory Control TLV may be used to indicate control information for reserved and lock areas. Contiguous and alternating lock and reserved areas may be indicated by a single Memory Control TLV.

Below the encoding of the 3 TLV fields of Memory Control TLV are shown:

T shall be equal to 02h.

L shall be equal to 03h.

V shall be composed of 3 bytes that uniquely identifies the position and the size of the reserved area. The 3 bytes shall be encoded in the following way:

- Position, MSB of the reserved Area field. It codes the position inside the tag of the reserved area. The Position byte consists of 2 parts (to calculate the bytes address from the position byte see below):
 - o PagesAddr, most significant nibble, coded as number of pages (0h=0...Fh=15) and
 - o ByteOffset, least significant nibble, coded as number of bytes (0h=0...Fh=15).
- Size, middle byte, coded as number of bytes (1h=1, FFh=255, 0h=256). It indicates the size in bytes of the reserved area.
- Partial Page Control, LSB. The partial page control provides the size in bytes of a page. It is split up into two nibbles of 4 bits each:
 - o BytesPerPage nibble: least significant nibble, coded as 2^n (0h=RFU, 1h=1...Fh=15). It indicates the number of bytes per page.
 - o Most significant nibble is RFU.

The byte address (ByteAddr) of each reserved area shall be calculated in the following way:

$$\text{ByteAddr} = \text{PageAddr} * 2^{\text{BytesPerPage}} + \text{ByteOffset}$$

The page definition has nothing to do with the block definition used by READ and WRITE commands. The block has a fixed size equal to 4 bytes instead the size of a page is defined by BytesPerPage field.

The NDEF Message TLV shall be always present inside the Type 2 tag. It stores the NDEF message inside the Value field. The NFC Forum Device shall be able to read/process the first NDEF message found; anyhow further NDEF Message TLV blocks MAY be present. Below the encoding of the 3 TLV fields of NDEF Message TLV is shown:

T SHALL be equal to 03h.

L SHALL be equal to the size in bytes of the stored NDEF message.

V SHALL store the NDEF message.

The Terminator TLV may be present inside the Type 2 tag, and an NFC Forum Device shall be able to read/process it. According to the type 2 tag operation specification of the NFC forum, the Terminator TLV is the last TLV block in the data memory area.

5

Terminator TLV shall be composed of 1 byte tag field. Below the encoding of the tag field of the Terminator TLV are shown:

T SHALL be equal to FEh.

L SHALL NOT be present.

10

V SHALL NOT be present.

Fig. 2 shows a data structure which can be read and written in accordance with an embodiment of the invention. In a header data block, configuration data including e.g. a tag unified identifier, lock bytes and manufacturer bytes may be stored. After the header data block, an application memory is located. Therein, application or user data can be stored in the form of one or more NDEF message TLVs. Additionally, a memory control data block can include reservation indicators for indicating a reserved partial memory area. In the type 2 tag protocol, this feature can be implemented by the memory control TLV. Behind the application data block, a terminator data block is located. It includes a Terminator TLV indicating to a NFC Forum Device the last byte of valid data in the application data block.

According to the type 2 tag protocol, the reserved memory area and the memory area after the Terminator TLV is not used and a NFC Forum device is adapted to jump over the reserved memory area and to stop any read/write operation at the location of the Terminator TLV. The non-used memory area of the reserved memory area is exploited by this embodiment of the invention to store additional data (called in the picture Any Data 1 and Any Data 2). This reserved memory area is sometimes also referred to as "fake reserved memory area".

In the example in fig.2 the NDEF Message TLV is split by a fake reserved memory area that contains Any Data 1 and Any Data 2. The NDEF Message TLV may be written several times. However its changes do not affect the Any Data 1 and Any Data 2 inside the reserved

memory area. According to the present embodiment Any Data 1 and Any Data 2 may also be modified but it should fit inside the reserved memory area.

The indication of the existence of the additional data in the reserved memory area may be:

- 5 - contained inside any NDEF Message TLV, or Proprietary TLV stored before the Terminator TLV,
- implicitly given from the position and size of the reserved memory area inside the contactless tag using the Memory Control TLV, or
- indicated by the unique identifier of the tag and any information related to the tag itself and
10 not to the data stored in it.

In the example of figure 2 the indication of the existence of Any Data 1 and Any Data 2 is implicitly given by the Memory Control TLV.

- 15 There might be one or more fake reserved memory areas with additional application data. Each fake reserved memory area might contain one or more even non-contiguous chunks of data that in the example are called Any Data 1, and Any Data 2.

The number, size and/or position of the chunks inside the fake reserved memory area may be
20 indicated:

- inside any NDEF Message TLV, or Proprietary TLV,
- inside any fake reserved memory area,
- by any application, or
- implicitly by the unique identifier of the tag and any information related to the tag itself and
25 not the data stored in it.

The fake reserved memory areas with additional data may be located anywhere inside the tag memory area after and also before the Terminator TLV. However, if a NFC Forum device is to be used, the rules described in the Type 2 Tag protocol concerning the reserved memory
30 area location inside a tag must be respected.

Fig. 3 shows a data structure which can be written and read in accordance with another embodiment of the invention. Therein, the fake reserved memory areas may be replaced using the dynamic lock bit areas. These ones are indicated using the Lock Control TLV. The

advantages and the indication of additional data using the dynamic lock bit areas are similar to that ones related to the fake reserved memory areas.

5 The only difference is when the contactless tag changes its state from READ/WRITE to READ_ONLY operation performed by a NFC Forum compliant reader device. In this case all lock bits must be set to 1b i.e. the additional data inside the dynamic lock bits areas is completely lost.

10 The invention can be used to be backward compatible with existing infrastructure like reader devices already deployed but at the same time to provide new additional features.

15 It should be noted that the term “comprising” does not exclude other elements or steps and the “a” or “an” does not exclude a plurality. Also elements described in association with different embodiments may be combined. It should also be noted that reference signs in the claims should not be construed as limiting the scope of the claims.

In order to recapitulate the above described embodiments of the present invention one can state:

20 The “Type 2 Tag Operational” draft specification shows how to store data inside a specific type of contactless cards or tags. This invention provides an additional way to store data inside the tag. It may be used for example to extend the memory area of new application versions, remaining backward compatible with the old ones. Moreover it provides a way to store data inside the tag data that cannot be seen by an NFC Forum reader device. This
25 functionality may be used to store any kind of data in any kind of format. For example this allows storing data without the overhead proposed by the type 2 tag protocol and NFC Data Exchange Format (NDEF).

30 The invention provides an additional method to store data inside any contactless card or tag compliant to the type 2 tag protocol. It is intended for any NFC Forum Device e.g. mobile phones, PDA, that stores data inside NFC Forum Type 2 Tags.

Possible advantages of this solution are inter alia:

- exploitation of non-used memory area: the data is stored in non-used memory area of the Type 2 Tag,

5 - capability to hide data in non-used memory areas being not visible using NFC Forum compliant reader devices,

- an NFC Forum compliant reader device may write data in the non-reserved areas without modifying the reserved memory areas.

10 - the method can be used by NFC Forum application that need an additional memory area to store data without touching the one defined by the NFC Forum standardization e.g. due to backward compatibility reasons.

The invention is applicable inter alia to:

15 - all contactless tags compliant to the "Type 2 Tag Operational" specification draft of the NFC Forum, and

- any data structure that follows that one specified by the "Type 2 Tag Operational" specification draft of the NFC Forum.

CLAIMS

1. A method for storing data in a memory array of a transponder, wherein a data structure for
5 storing data within the memory array is defined by a predetermined protocol, the data
structure comprising:

a header data block including predefined header data;

10 an application data block for storing application data; and

a memory control data block including a reservation indicator for indicating a reserved partial
memory area of the memory array where, in accordance with the predetermined protocol,
application data cannot be read or written by a protocol compliant reader device;

15

the method comprising:

storing additional application data in the reserved partial memory area.

20 2. The method according to claim 1, further comprising storing a storage indicator for
indicating that additional application data is stored within the reserved partial memory area
wherein the storage indicator is stored in at least one of the header data block, the application
data block and the memory control data block.

25 3. A method for reading data in a memory array of a transponder, wherein a data structure for
storing data within the memory array is defined by a predetermined protocol, the data
structure comprising:

a header data block including predefined header data;

30

an application data block for storing application data; and

a memory control data block including an reservation indicator for indicating a reserved partial memory area of the memory array where, in accordance with the predetermined protocol, application data cannot be read or written by a protocol compliant reader device;

5 the method comprising:

reading additional application data stored within the reserved memory area.

10 4. The method according to claim 3, further including searching for a storage indicator stored in at least one of the header data block, the application data block and the memory control data block, wherein the storage indicator includes data for indicating that additional application data is stored within the reserved memory area.

15 5. The method according to one of claims 2 or 4, wherein the storage indicator comprises at least one of data indicating a storage address, a field length, a number of fields and a type of application data stored in the reserved memory area, wherein the method is performed taking into account at least one of these data.

20 6. The method according to one of claims 1 to 5, wherein the reservation indicator included in the memory control data block causes a protocol compliant reader device to jump over the indicated reserved partial memory area when storing or reading data in the memory array.

25 7. Method according to one of claims 1 to 6, wherein the reserved memory area is positioned within the application data block.

8. The Method according to one of claims 1 to 7, wherein the predetermined protocol is the Type 2 Tag Operation specification of the NFC Forum.

30 9. Transponder in which data is stored in accordance with one of claims 1 or 2 or one of claims 5 to 8 when referred to one of claims 1 or 2.

10. Read/write-device adapted to perform the method according to one of claims 1 to 8.

11. A computer readable medium including a program element adapted to perform the method according to one of claims 1 to 8.

12. A program element adapted to perform the method according to one of claims 1 to 8.

5

10

Byte Number	0	1	2	3	Block
UID / Internal	UID0	UID1	UID2	Internal0	0
Serial Number	UID3	UID4	UID5	UID6	1
Internal / Lock	Internal1	Internal2	Lock0	Lock1	2
CC	CC0	CC1	CC2	CC3	3
Data	Data0	Data1	Data2	Data3	4
Data	Data4	Data5	Data6	Data7	5
Data	Data8	Data9	Data10	Data11	6
Data
Data
Data
Data
Data	n
Lock / Reserved
Lock / Reserved
Lock / Reserved	k

Fig 1

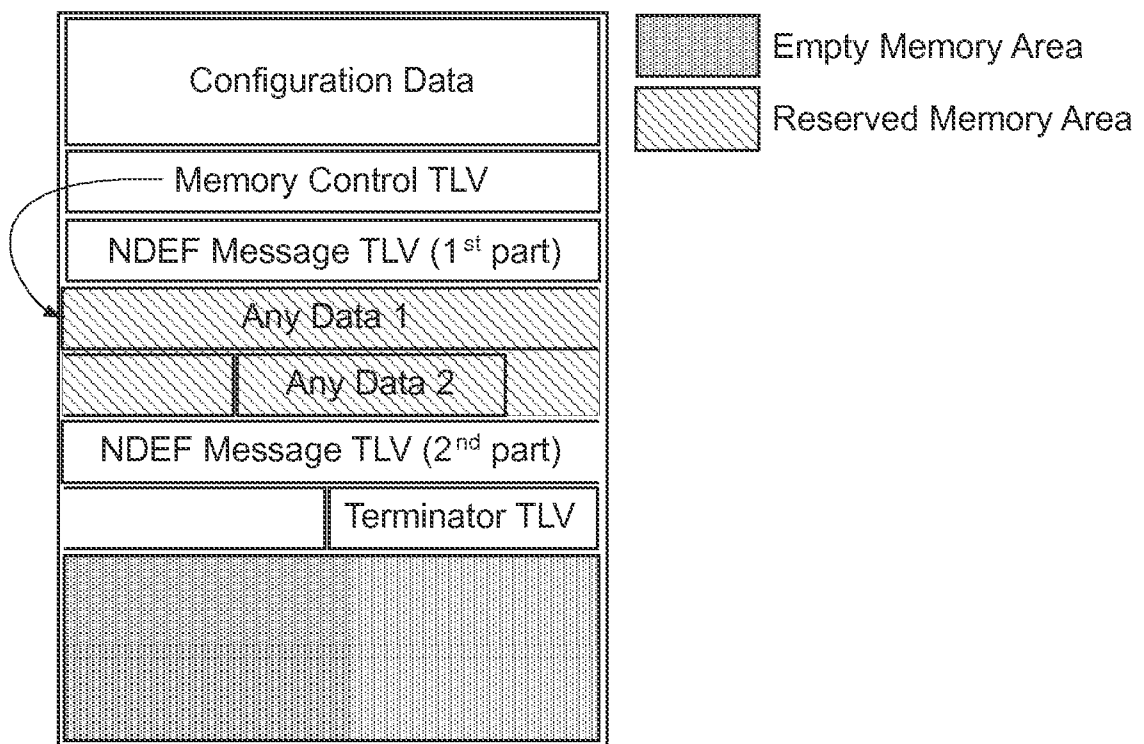


Fig 2

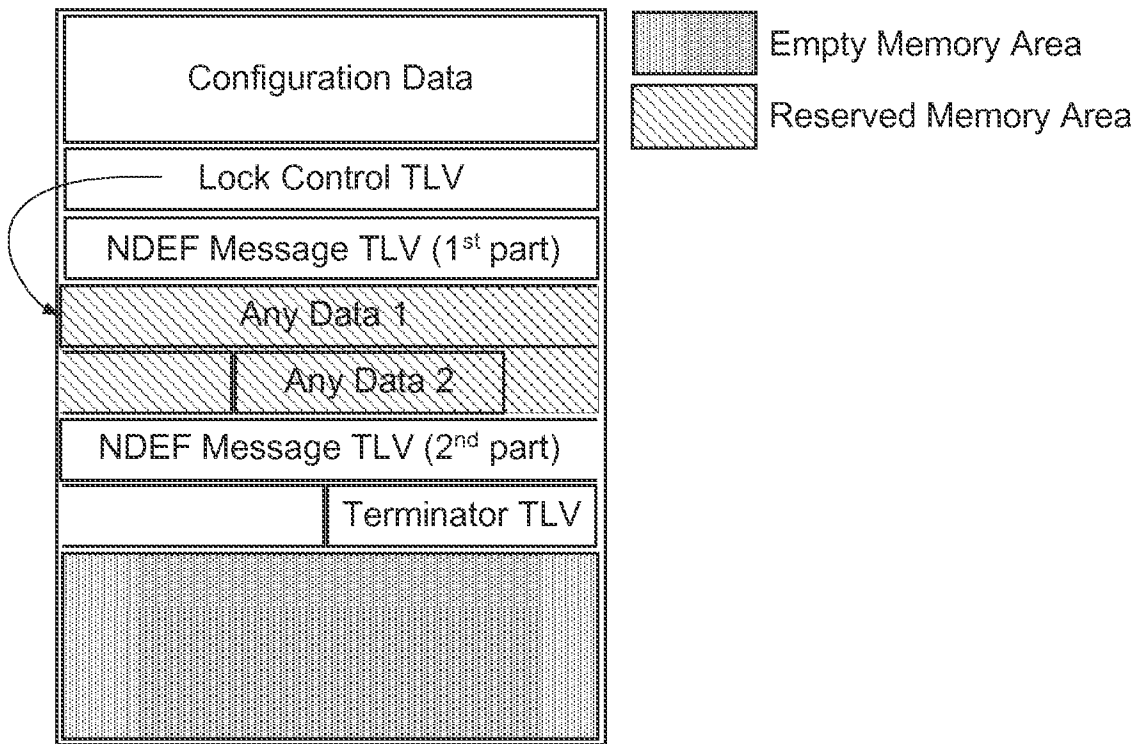


Fig 3