INTERNATIONAL STANDARD

ISO 20910

First edition
2019-08

Coding for radio frequency identification (RFID) tyre tags

Codage de tags d'identification des pneumatiques par radio fréquence (RFID)

Reference number
ISO 20910:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 31, *Tyres, rims and valves.*

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document describes data construction best practices, processes and methods for tyre identification, verification, traceability and product characteristics. An extensive effort has been undertaken to make data interchangeable between 2D (e.g. Data Matrix/QR Code) optical symbols and electronic media like RFID to permit the user to select the appropriate technology with a minimum impact on information technologies (IT) infrastructures. These technologies complement each other and may be used jointly or separately as the application can require. This document is focused on the application of RFID to achieve these ends.

The provisions in this document are intended to express the minimum requirements for passive RFID tags and are not intended to limit the development of the technology in the future.

This document also provides guidance to tyre manufacturers on using RFID tags for tyre identification during the manufacturing process or in the aftermarket (i.e. RFID patch application) in tyres, service life and for other purposes. Tyre dealers and retreaders may also use RFID tags for inventory and retread control of tyres, and fleets may use them for tyre record keeping, tyre performance analysis, maintenance and inventory control.

The use of an RFID tag in tyre application follows strict rules in order that the data format can be used globally within the tyre and transportation industries.

This standardization will allow for interoperability and the use of interchangeable hardware and software from multiple suppliers resulting in greater efficiencies.

This document:

— specifies the air interface standards required between the RFID interrogator (also known as a reader) and RFID tag;

— specifies the use of industry recognized GS1 codes;

— clarifies the role of the company prefix;

— specifies the semantics and data syntax to be used in the data construction for MB01;

— provides a unique item identifier for traceability (UII, stored in MB01);

— provides information on the use of the UII in MB01 as the link to database infrastructures;

— specifies the option for user memory bank (MB11).

This document is based on the requirements in the following:

— technology: only passive ultra high frequency (UHF) RFID tags are used;

— global interface: the air interface protocol is ISO/IEC 18000-63, which is equivalent to GS1 EPC Gen2 V2.0.1.

A unique item identifier (UII) is not the same as a part number, a DOT tire identification number (TIN), a CCC code, a branded ID, or other names for tyres. Foremost in making an ideal UII is to know who made the part. Because of this, the UII is often referred to as the “birth record”. A constraint with internally-derived numbering schemes is that they are only unique to the domain owner; they may have duplicates within the “world”, and rarely communicate intelligently who the owner actually is (outside of their domain). In order to clearly identify who, there must be a globally recognized register of companies. That is where GS1 play a key role.

The international role of the GS1 is to register companies and issue assigned company prefixes, much the same way that cell phones have assigned company IDs as provided by international telecommunications agencies.

Coding for radio frequency identification (RFID) tyre tags

1 Scope

This document specifies the terms and definitions, general requirements and data structure for coding radio frequency identification (RFID) tyre tags.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18000-63, *Information technology — Radio frequency identification for item management — Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C*

ISO/IEC 19762, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

ISO 20909, *Radio Frequency IDentification (RFID) tyre tags*

GS1 EPC™ Tag Data Standard[1)]

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 and ISO 20909 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
memory bank
MB
designated name of a segmented memory structure

Note 1 to entry: ISO/IEC 18000-63 compliant tags have 4 (four) individually usable memory banks, numbered Memory Bank 00(MB00), Memory Bank 01(MB01), Memory Bank 10(MB10), Memory Bank 11(MB11). See Table 1.

3.2
company prefix
CP
number code of the tyre manufacturer provided by GS1 and encoded in SGTIN

1) This standard defines the Electronic Product Code™, and also specifies the memory contents of Gen 2 RFID Tags. In more detail, the Tag Data Standard covers two broad areas: the specification of the Electronic Product Code, including its representation at various levels of the EPC global Architecture and its correspondence to GS1 keys and other existing codes, and the specification of data that is carried on Gen 2 RFID tags, including the EPC, "user memory" data, control information, and tag manufacture information.

3.3
global trade item number
GTIN
unique identifier for trade items used to look up product information in a database

3.4
serial number
number indicating place in a series and used as one of the components of the *unique item identifier* (3.6)

3.5
serialized global trade item number
SGTIN
electronic product code (3.7) including *GTIN* (3.3) and *serial number* (3.4) of a single trade item

3.6
unique item identifier
UII
birth record
unique identifier for a physical item that in this case is a tyre

Note 1 to entry: It refers to the unique identifier written into MB01 of the tyre RFID in this document.

Note 2 to entry: Item refers to products, transportation units, recyclable assets and services.

3.7
electronic product code
EPC
globally unique *serial number* (3.4) that identifies an object in the supply chain

Note 1 to entry: EPCs are administered by GS1.

3.8
lock
locking
ability of the tag protocol to cause:

— the reserved *memory bank* (3.1) MB00 to be read and write protected,

— the UII memory bank MB01 to be write protected,

— the user memory bank MB11 to be write protected

Note 1 to entry: Once "locked," that memory bank can only be changed back to "readable / writable" by using the access password.

3.9
permalock
ability of the tag protocol to cause a *memory bank* (3.1) to be locked permanently

Note 1 to entry: Once "permalocked," that memory bank cannot be unlocked whatever the access password.

3.10
Tag ID
TID
globally unique serialized identification of the individual silicon chip programmed and locked by the silicon manufacturer

4 General requirements

4.1 Memory banks and data structure organization

This clause defines details for tyre application.

Data structure organization shall conform to protocol ISO/IEC 18000-63.

Data structure organization divides the tag memory storage into (four) memory banks (see Table 1) which are represented in Annex A.

Table 1 — Memory bank use

Binary	Memory bank	Use
00	RESERVED	This memory bank is the password management memory bank and contains access password and kill password.
10	TID	TID is unique part and serial number of the RFID tag and permanently locked by the chip manufacturer. This memory bank is not used by tyre manufacturers and is locked by chip manufacturer. It is not described in this document.
01	UII	The unique item identifier is written within this memory bank under the responsibility of the tyre manufacturer.
11	User memory	The user memory is optional. Whenever available, stakeholders can use it under their own responsibility.

4.2 UII memory bank (MB01)

For tyre applications, UII shall be coded using SGTIN-96 (96 bits - serialized global trade item number) as per GS1 EPC Tag Data Standard.

The size of MB01 is limited and its purpose is to contain the name (UII, birth record) by which the Tag (and the tyre to which it is associated) is known.

The UII in MB01 is programmed one time when the tag is commissioned and then the content of MB01 is permalocked. This is the information used for asset identification, control and tracking purposes and accessibility to authorized databases remotely or on a local device.

It is the responsibility of the tyre manufacturer installing and programming the tag's birth record (the process is known as "commissioning") to properly follow the rules for "naming" the tyre and placing that information into the UII section of MB01.

Once commissioned, the UII shall remain unchanged within the tag.

4.3 RFID technical specification

4.3.1 UII memory bank MB01 size

For tyre application, the minimum size of the UII memory bank MB01 shall allow 96 bit SGTIN encoding.

4.3.2 Security/Locking data (Permalock command)

The kill function shall be disabled before leaving the tyre manufacturer facilities in accordance with ISO/IEC 18000-63. Kill password has to be set to 00000000h and permalocked.

Once the UII data has been written into MB01, this memory bank shall be permalocked.

The access password can be either:

— unlocked (readable), or

— locked or permalocked (unreadable).

The latter may mean that there is additional information regarding the product in the user memory bank (MB11) or in a database. In that case, UII (SGTIN 96) only refers to the original casing of the product and might not be directly decoded as the product identity anymore.

In the case of retreaded tyres, the retreader can lock (or permalock) the access password (if this has not already been done by another stakeholder). This should make the reader aware that additional information (about the retreader) can be found in a database. The content of UII memory bank MB01 (encoded with SGTIN 96), that only refers to the original casing of the product, might not be directly decoded as the product identity anymore.

4.3.3 Numbering system identifier

Bit 17_h of the stored PC shall be set to 0 in order to conform to GS1 EPC Global requirements.

5 Memory banks

5.1 MB00 (Reserved memory bank)

MB00 is the password management memory bank that contains:

— access password,

— kill password.

5.2 MB01 (UII memory bank)

MB01 is UII memory bank, which contains the following data:

— CRC: calculated 16 bits checksum on the tag for data verification on the air interface from address 00_h to $0F_h$;

— stored PC, a 16 bits protocol control word which contains several data fields, including:

  — L: length of the UII stored in 10_h–14_h,

  — T (numbering system identifier toggle, bit 17_h): bit 17_h has to be set to 0_2 as per GS1 EPCglobal™[2)] application and PC bits 18_h – $1F_h$ shall be as defined in this protocol,

  — UII field: contains the UII starting at address 20_h.

5.3 MB10 (TID memory bank)

TID is a unique part and serial number of the RFID tag and is permanently locked by the chip manufacturer.

5.4 MB11 (User memory bank)

The MB11 is optional. Whenever available, stakeholders can use it under their own responsibility.

2) This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named.

6 Data structure for unique item identifier (UII)

The minimal data elements to meet item identification shall follow the GS1 EPC Global Coding Scheme for Item Identification (SGTIN-96) (see Table 2 and Table 3); Identification of the tagged object is accomplished via the UII.

A 96-bit UII (SGTIN-96) shall be used and permalocked after commissioning.

Table 2 — Data structure in MB01

	UII					
EPC GS1 SGTIN-96	Header	Filter value	Partition	Company prefix	Item reference	Serial number
Length (bits)	8	3	3	20 to 40	24 to 4	38
Example						
Value (binary)	0011 0000	000	010 (for 34 bits GS1 Company prefix and 10 bits item reference)	010...01 (34 bits)	010...01 (10 bits)	010...01 (38 bits)

The SGTIN-96 format consists of the following data fields and has an overall length of 96 bits:

— header (8 bits): definition of the coding scheme, in which the structure and length of the actual EPC identifier are defined (e.g., SGTIN-96, global returnable asset identifier (GRAI), etc.). SGTIN-96 header value shall be $0011\ 0000_2$;

— filter value (3 bits): provides a fast filtering to determine the item basic category. In this document, the filter value is 000_2 since tyre belongs to "other item" category;

— partition field (3 bits): contains a code that indicates the number of bits in the GS1 company prefix field and the indicator/item reference field;

— company prefix (20 – 40 bits): assigned by GS1 to a managing entity. The company prefix is the same as the company prefix digits within a GS1 GTIN in binary code;

— item reference (24 – 4 bits): assigned by the managing entity to a particular object class. The item reference for the purposes of EPC encoding is derived from the GTIN by concatenating (i.e. linking) the indicator digit of the GTIN and the item reference digits and treating the result as a single integer;

— serial number (38 bits): assigned by the managing entity to an individual object as a single integer.

UII (EPC) coding scheme for item based on GS1 SGTIN-96 is shown in Table 3 (IAC is GS1).

NOTE The structure of Table 3 follows GS1 EPC Gen2 V 2.0.1 and it is up to the entity applying this document to verify the compliance with the latest version of GS1 EPC UHF Gen2 Air Interface Protocol.

Table 3 — EPC coding scheme for item based on GS1 SGTIN-96

	Bit location (hex)	Data type	Example value (binary)	Size (bits)	Description
CRC + PC word	00-0F	CRC	Computed	16	Cyclic redundancy check
	10-14	Length	00110	5	Represents the number of 16-bit words comprising the PC field and the Reserved/AFI field, 001102 corresponds to 6 words.
	15	UMI	Computed	1	May be fixed by the tag manufacturer or computed by the tag 0_2 = No valid user data, or no MB11 1_2 = Valid user data in MB11
	16	XI	Computed	1	XPC_W1 indicator
	17	T	0	1	As bit X17 is 0_2 then the application is referred to as a GS1 EPCglobal™ Application and PC bits X18-X1F shall be as defined in this protocol.
	18-1F	RFU	0000 0000	8	Reserved for future use
	Subtotal			32	
UII	20-27	Header	0011 0000	8	Definition of coding scheme (SGTIN-96)
	28-2A	Filter	000	3	The filter value is additional control information that may be included in the EPC memory bank of a Gen 2 tag. The intended use of the filter value is to allow an RFID reader to select or deselect the tags corresponding to certain physical objects.
	2B-2D	Partition	Up to GS1 or tyre manufacturer	3	Indicates the number of bits used for both GS1 company prefix and item reference number
	2E-(41 to 55)	GS1 company prefix	Up to GS1 or tyre manufacturer	20 to 40	See GS1 general specifications for more detail on how to construct GS1 company prefix
	(42 to 56) - 59	Item reference number	Up to GS1 or tyre manufacturer	24 to 4	Part number identifier
	5A-7F	Serial	Up to tyre manufacturer	38	Serial number (2^{38} different values)
	Subtotal			96	
NOTE Maximum decimal value range of company prefix and item reference fields varies according to the contents of the partition field.					

Table 3 *(continued)*

	Bit location (hex)	Data type	Example value (binary)	Size (bits)	Description
	Total			128	
NOTE Maximum decimal value range of company prefix and item reference fields varies according to the contents of the partition field.					

Annex A
(informative)

Data scheme for tyre RFID tag

A.1 Tag memory mapping

Passive UHF tags that are compliant with either ISO/IEC 18000-63 or EPC Class1 Gen2 standards have a physical memory that is logically separated into the four distinct memory banks. Each of the memory banks can be addressed separately. Any operation on one of these memory banks shall not impact other memory banks. An exception is a possible change to the memory bank sizes, which are linked to each other.

The logical addressing of all memory banks shall begin at 00_h. The physical memory map is tag-manufacturer defined.

The memory banks are:

— **Reserved memory bank (MB00)** contains the kill and access passwords. These passwords allow to implement kill and access commands. In order to use these commands, corresponding passwords have to be set to a value that is not 00000000_h. Unless otherwise stated, tag manufacturers deliver tags with access and kill passwords set to 00000000_h.

  The kill password is stored at memory addresses 00_h to $1F_h$ and the access password is stored at memory addresses 20_h to $3F_h$ of the MB00.

  In order to make a tag unkillable, kill password has to be set to 00000000h and permalocked. In that way, the kill function that requires a kill password different from 00000000h can never be invoked.

— **EPC memory bank (MB01)** contains a stored CRC at memory addresses 00_h to $0F_h$, a stored PC at addresses 10_h to $1F_h$, an identifier (such as an EPC, and hereafter referred to as an EPC) that identifies the object to which the tag is or will be attached beginning at address 20_h.

  In case the tag implements extended protocol control (XPC) then either one or two XPC word(s) are stored at address beginning at 210_h.

— **TID memory bank (MB10)** contains an 8-bit ISO/IEC 15963 allocation class identifier at memory locations 00_h to 07_h. TID memory bank may also contain additional identifying information above 07_h so that an interrogator can uniquely identify the custom commands and/or optional features that a tag supports.

  This information is encoded and permalocked by the chip manufacturer so that it cannot be changed.

— **User memory bank (MB11)** is optional. If a tag implements user memory then it may partition it into one or more files. If the tag implements a single file then that file is File_0.

Figure A.1 summarizes the bits allocations. More information can be found in ISO/IEC 18000-63:2015, 6.3.2.

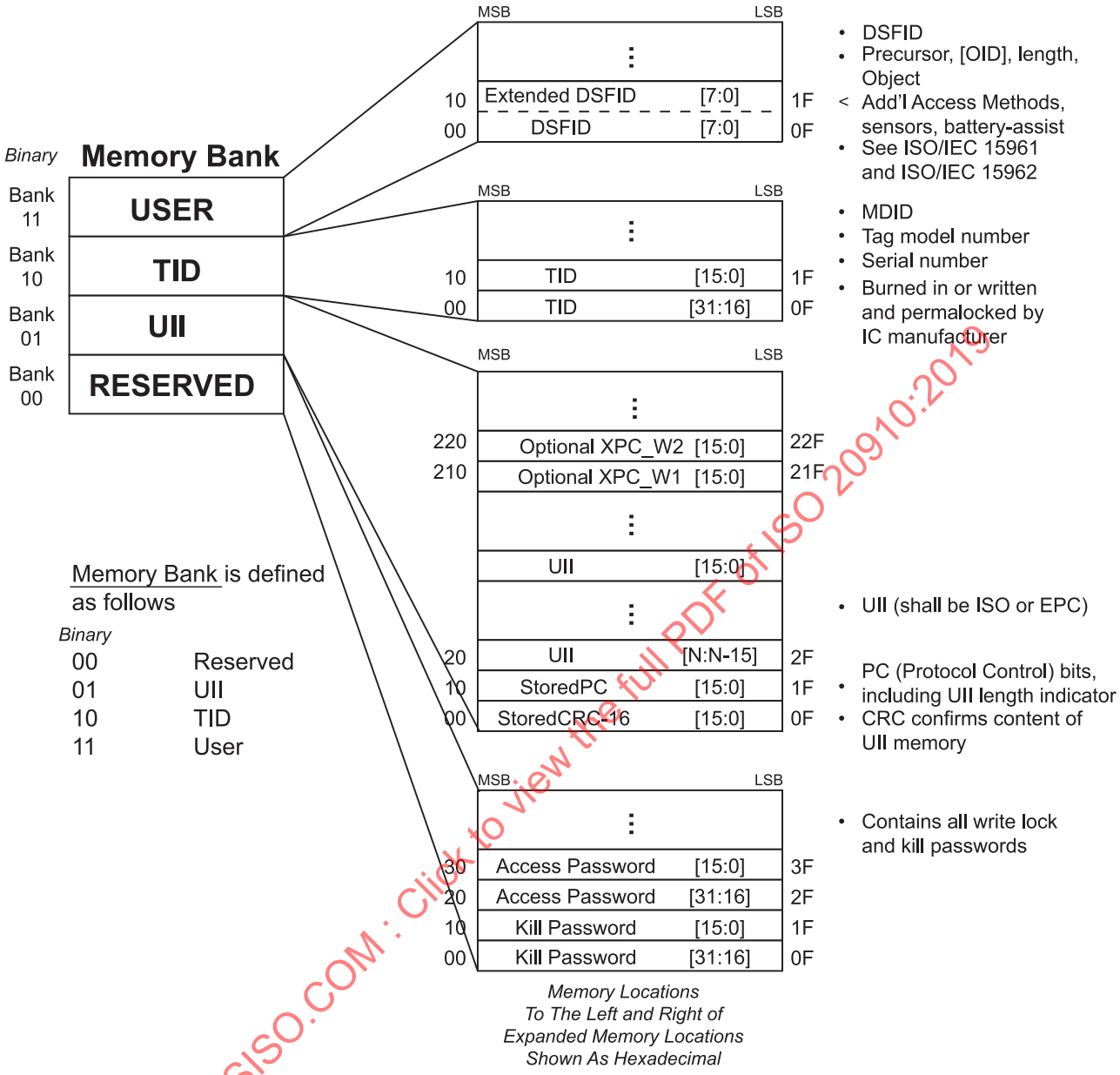

Figure A.1 — Memory banks of UHF passive RFID tag

A.2 Main mandatory and optional commands

A.2.1 Basic operations

Select: allows to select a particular set of tags before inventory. This selection can be made on different parts of the memory banks. This allows to reduce the number of tags that will be inventoried to those that are of interest.

EXAMPLE Reader can select only tags that have a particular value of the EPC memory bank (e.g. the tags that only have a particular value of the company prefix in the SGTIN-96 EPC memory).

Inventory: allows to make the inventory of all selected tags. Once inventoried, the tags will backscatter their EPC.

Access: allows to communicate with one particular tag that has been previously inventoried.

A.2.2 Access commands (OPEN or SECURED state)

Read (mandatory): this sccess command allows the reader to read part or all tag's reserved, EPC, TID or user memory banks.

Write (mandatory): this access command allows the tag memory location to be changed. This concerns reserved, EPC, TID and user memory banks. Any locked memory location cannot be changed without the right access password. Any permalocked memory location cannot be changed.

Parameters are: handle (RN16) (The pointer to a particular tag in a list of inventoried tags), MemBank (memory to access), WordPtr (address to be written), Data (16 bits word to write), CRC-16 (CheckSum).

In EPC Class1 Gen2 V2.0.1, data can be sent cover-coded or encrypted.

Kill (mandatory): this access command will permanently disable a tag. This is a 2-stage command:

— containing the cover coded 16 MSB of the kill password,

— containing the cover coded 16 LSB of the kill password.

Before each kill command, a new handle is requested and in response to a kill command, the tag backscatters its handle and never responds again.

If kill password is 0 (default setting), a tag cannot be killed.

Lock (mandatory): this access command allows a reader to:

— lock individual passwords, preventing subsequent reads or writes;

— lock individual memory banks, preventing subsequent writes.

— permalock (permanently lock) the lock status of passwords or memory banks.

Permalock bits, once set, cannot be changed. The lock bits cannot be read directly but inferred by other memory operations. The tag will indicate success, error or failure and the tag has to be in secured state for the command to be accepted.

If the passwords are locked or permanently locked then they are unwriteable and unreadable by any command and usable only by a *kill* or *access* command.

If EPC memory, TID memory, or File_0 are locked or permanently locked then they are unwriteable but readable, except for the **L** and **U** bits in EPC memory that are reserved respectively for the length of the UII and for optional untraceable command.

Access (optional): this optional command allows a reader to transition a tag with a non-zero access password, from an open to a secured state.

BlockWrite (optional): this optional command allows a reader to write multiple blocks to a tag's reserved, EPC, TID or user memory banks. Data cannot be sent encrypted.

BlockErase (optional): this optional command allows a reader to erase multiple blocks to a tag's reserved, EPC, TID or user memory banks.

BlockPermalock (optional): this optional command allows to permanently lock one or more memory blocks. If blocks within File_0 are permalocked then these blocks are permanently unwriteable but readable. If blocks within File_N, N>0 are permalocked then these blocks are permanently unwriteable but readable by an interrogator with appropriate read privileges.

Authenticate (optional): allows an interrogator to perform tag, interrogator, or mutual authentication. The generic nature of the authenticate command allows it to support a variety of cryptographic suites.

AuthComm (optional): allows authenticated communications from reader to tag by encapsulating another command in the AuthComm's message field.

