RAIN Item Numbering and Tag Data

RAIN RFID Alliance
Technical Note

V.1.0

July 2020

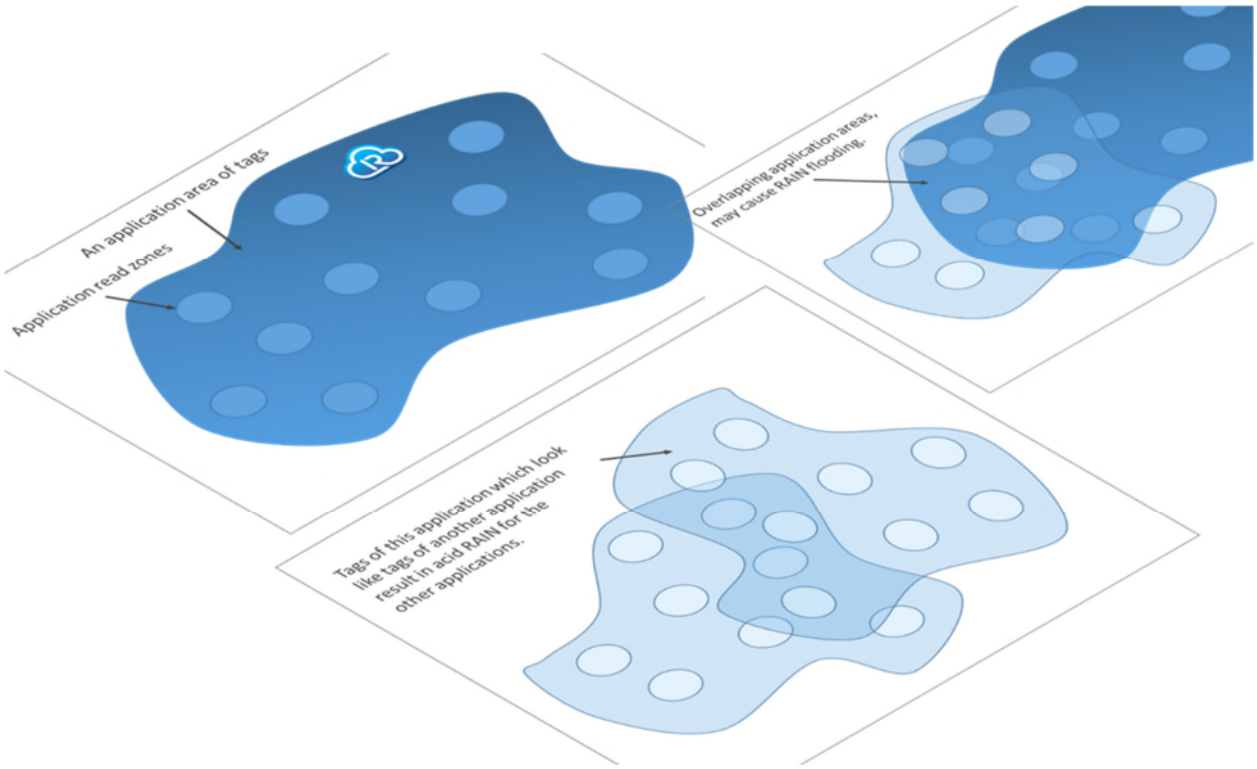
RAIN RFID Technical Note: RAIN Item Numbering and Tag Data

The purpose of this technical note is to describe the potential of RAIN tag use at the hand of the different types of RAIN tag data elements, each with its purpose, benefits, and issues.

The aim is to inform business leaders, integrators, and users of the advantages of proper usage of RAIN item/object numbers and its data as stored in its tag. This also addresses the critical issues of 'RAIN flooding' (occasions where too many tags are in the read zone) and 'acid RAIN' (occurrences of poorly programmed tags and of tag cloning/copying).

This technical note discusses RAIN tag data from a business perspective, followed by a discussion of the tag data elements as seen/received by a data practitioner. It then provides a high-level overview on tag data access and integrity.

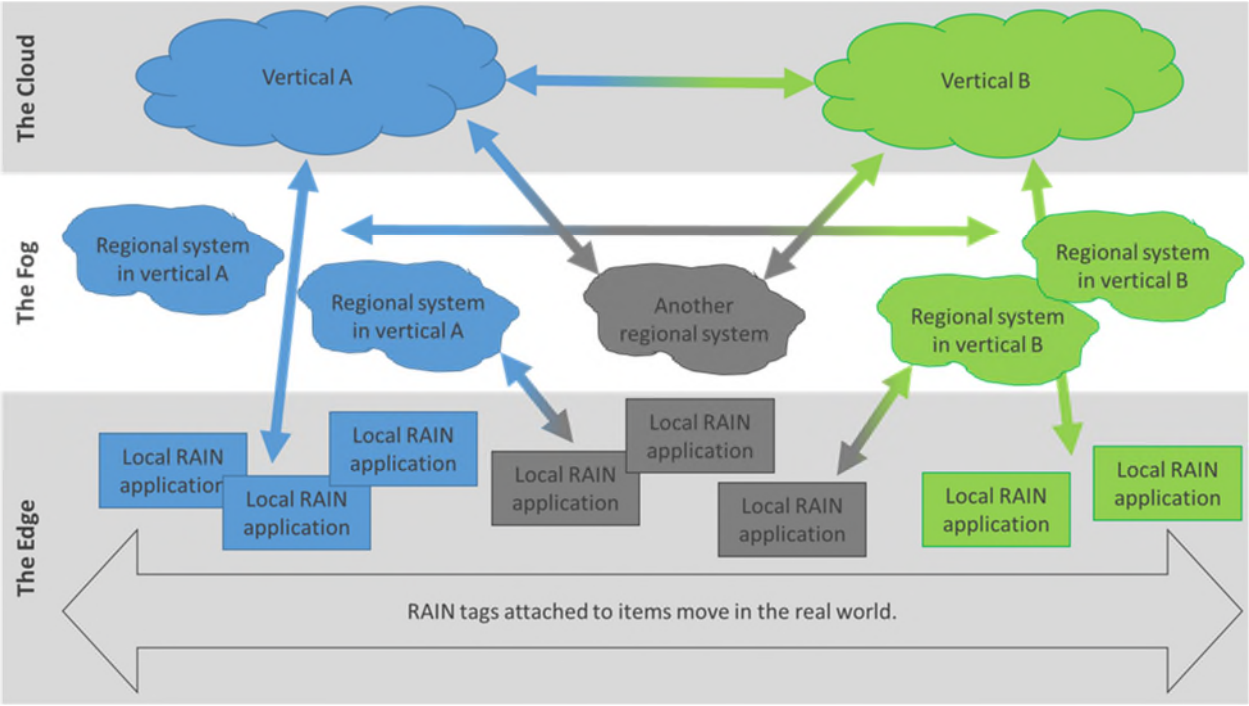
This technical note is aligned with the methods of the RAIN Reader Communication Interface (RCI) guide and the GS1 Low Level Reader Protocol (LLRP) as they provide access to the RAIN tag data and features using the RAIN air protocol standards (ISO/IEC 18000-63 and GS1 UHF Gen2 Air Interface). Relevant data standards are referenced where applicable.



Contents

1. RAIN Number and Tag Data

RAIN has experienced significant growth in recent years with 18 billion tags sold in 2019 alone. It has become a very successful automatic identification technology with systems being deployed in an increasing number of market verticals. More important is the convergence of verticals and the federation of RAIN RFID enabled systems resulting in spatial overlap of deployments. The number of small and medium RAIN enabled applications and services are growing rapidly, finding global appeal with a proven return on investment.



RAIN RFID distinguishes itself from other automated identification systems in its ability to inventory and access hundreds of tags simultaneously over distances of more than 10 meters in a very short time. This capability facilitates cost efficient automated item identification. In contrast, barcodes and NFC has a typical one tag - one reader relationship usually requiring manual operations or expensive dedicated readers, such as retail point of sale tills and baggage handling systems. Notably, the airline industry is recommending that baggage tags integrate RAIN RFID for this very reason with many global applications following this trend.

These highly efficient, long-range, multi-read features make RAIN RFID the ideal technology to identify real world items in the digital world. This power, however, must be wielded with discipline. The benefits of long range and multi tag reading can also cause interference between RAIN enabled applications and services.

RAIN tag interference between applications is known as Tag Pollution of which acid RAIN and RAIN flooding poses real long term issues. Notably, correcting errors in programmed tags in the field is an expensive operation in terms of money, time, and reputation. In contrast, RF interference can often be addressed through local engineering.

Acid RAIN: This describes a scenario where tags intended for use in one application impact the performance of another system where similar tag identification numbers are used. The result can be

chaotic when these tags appear in the read zone of the other system's readers. There is evidence of this already happening in the field and with the phenomenal success of the technology, Acid RAIN is expected to occur with increasing frequency.

Knowing which tag belongs to which application allows a specific application to target its tags and ignore all other tags.

RAIN Flooding: The time to read tags is limited. Some tags will not be read when too many of them are at the same time in the read zone. The number of tags in a read zone is becoming more unpredictable as RAIN deployments increases.

Knowing which tag belongs to which application allows a reader of a specific application to instruct only its tags to respond, all other tags shall stay silent.

To know your tags requires you to follow the tag data numbering standards!

For the success of YOUR application as well as all other RAIN applications YOU must use the appropriate numbering and data standards for YOUR RAIN tags.

1.1. Object identifier specification

The item/object identifier is the name of the item the tag represents. Get it wrong and chaos ensues (RAIN flooding and acid RAIN).

A standard tag object number contains an identifier of the owner/issuer of the tag data. Both GS1 and ISO use ISO/IEC 15459 for this purpose. The TID (the unique tag chip identifier) is sometimes used as the unique object identifier. The tag may also contain object information. See the annexes for details on tag memory.

The term **object** (which is more generic), as an alias for **item**, is used in the remainder of the document.

The object identifier can be specified with the following methods (the first two are recommended):

1. **Standard-managed** object number methods:
   - ISO object number schemes (unique item identifier - **UII**) are specified by the ISO/IEC 1736x series of standards or ISO/IEC 15961 registered global organisations, like IATA, specify, manage, and administer their own numbering system and data.
   - The widely adopted Electronic Product Code (EPC) encodings, standardised and maintained by GS1 and **specified in detail in the EPC Tag Data Standard (TDS)**.
2. **Self-managed** object number methods: ISO/IEC 20248 is an ISO item number scheme which allows ISO/IEC 15459 registered companies and organisations to develop, manage and administer their own item numbers and verifiable tag data structures.
3. **Proprietary** object number methods.

   PLEASE AVOID THE USE OF PROPRIETARY NUMBERS.

   Note, proprietary object numbers may result in acid RAIN.

If the use of proprietary object numbers is unavoidable, then use the ISO/IEC 15961 scheme with the Application Family Identifier set to PROPRIETARY; the tag set to ISO (PC bit T=1) and AFI set to 0x01, 0x02 or 0x03.

The use of standard tag data ensures that no tag data interference occurs.

1.2. Item information specification

The three methods to specify additional RAIN tag data (object information) are:

1. Registered data methods: The ISO Data Storage Format Identifier (DSFID) provides for data formats whereby object information data structures are developed, managed, and administrated by registered organisations. The DSFID formats are administered by the ISO Registrar AIM Inc. (ISO/IEC 15961).
2. Self-managed data methods: ISO/IEC 20248 has been assigned a DSFID (0x11) which allows ISO/IEC 15459 registered companies and organisations to develop, manage and administer their own verifiable data structures. It works with all numbering systems, be it, GS1, ISO or proprietary.
3. Proprietary data methods: encoding schemes are unilaterally and implemented by the system owner.

2. Types of RAIN tag data

The following section discusses tag data types and they are detailed in increasing order of complexity. The discussion also provides an indication of the infrastructure necessary to support each tag data type.

It should be noted that a specific tag represents a real-world object in the digital world, thus allowing systems to make decisions and take actions relating to the item.

The discussion assumes the following data layers:

- Cloud – interaction with tag and object data via cloud services.
- Fog – interaction with tags and objects via directly connected systems within regional related localities.
- Edge – interaction with tags and objects at a singular locality and typically, but not necessarily, by a single system/application.
- Reader – RAIN RFID infrastructure used to interact with the tag.
- Tag – RAIN RFID data carrier representing a specific object.
- Tag issuer – the point where tags are programmed (i.e. personalized).

Note, tag information may be changed during the lifecycle of the item and its tag. The item identification data (item number) on a tag should however not be changed. It is highly recommended to lock the UII/EPC memory bank (MB01).

In open and Internet of Things (IoT) systems various entities contribute infrastructure components and often share data; for example, machine parts might be tagged by the manufacturer intended for use in operations and by an independent maintenance provider. GS1 EPC tags are typically issued by the item manufacturer but also used by different operational verticals such as freight, logistics, stock, and sales, potentially all different entities. This is commonly known as federation[1] of data as practised by IoT enabled "smart" system environments.

Closed and proprietary systems typically own and operate all data and system components in a vertical, i.e. the same entity will issue, read and use the tag data.

Systems use various methods to identify objects and store related information. The following numbering methods are available:

1. Digital Twin tags where the object's identity and all related information is stored in a cloud, often called a Digital Twin of the object. The tag only contains a unique identifier used as a reference to the object information and the cloud where it is stored.
2. Identification tags where the numbering system is standardised to enable Fog and Edge item identification.
3. Information tags where the tag also contains information about the object to enable Fog and Edge operations where connectivity is restrained.

Both the level of openness of an application, and reliability of connectivity play an important role in the choice of tag data methods.

A closed application is deployed, managed, and operated by a single entity with line accountability to a single authority.

2.1. Digital twin tags

A digital twin is a tag that uses a unique number to point to a record in the cloud which contains all the information about the tag and the object it represents. This information may include a description of the object, current status, and ownership, and its full history. The unique number encoded on the tag is often random to prevent mass-downloads of data and to reduce the possibility of predicting object codes.

When compared to tags designed to hold more data or functionality, these tags are typically less expensive and fastest to read; but the data contained on the tag only becomes useful once the cloud has been accessed. Cloud data storage may be cheap when considered in isolation, but the costs associated with protecting, accessing, and sharing cloud data must be considered. Cloud data may not always be accessible or available in a timeframe appropriate to allow local decision making.

[1] "Federation" in data systems is a mechanism whereby a set of autonomous (both in instance and ownership) data sets and services, through a common set of data models, policies, practices and protocols, are offered as a composite data set and service. For example, a federated RAIN reader in a hospital reports tags to more than one autonomous system, which may be a device locality system, a device consumable management system and the general cleaning system. Federation is a very handy tool for IoT and Smart Cities, in fact all things Smart".

Digital twin tags are a good choice where deterministic cloud services are available at all tag read points and especially for close loop applications where a single entity has operational ownership of necessary infrastructure and processes.

An aim of promoters of digital twin tags is to construct and deploy a single digital twin tag cloud for all tags. Such a cloud will have many access points similar to the Domain Name Services (DNS) services. Such a single tag cloud will dissolve the acid RAIN issue completely, but the issue of RAIN flooding may become prevalent due to the latency and bandwidth required for both cloud lookups and information synchronisation. The problem of having 'too many tags in the read zone' may eventually become 'too many tags to cope with'.

Whilst technically a single digital twin tag cloud may be possible, the business and politically feasibility is more questionable; even when considering multiple industry or application specific digital twin tag clouds. For example, companies in competition will likely be uncomfortable to share a cloud for all their products. Similarly, the sharing of all vehicle registrations globally is currently inconceivable, even for collaborating countries. It is inevitable that many digital twin tag clouds will exist in parallel with other RAIN enabled services and applications.

It is physically difficult, and often impractical, to ensure that only the tags intended for use in one specific system will only ever appear in its read zones. Foreign tags in a read zone will become an increasing reality due to the growth in the RAIN tag population and the growth in RAIN enabled applications. The reader infrastructure of a digital twin tag system should have the ability to identify which tags are part of its system to prevent RAIN flooding and acid RAIN. A federated reader interested in digital twin tags from different clouds must know which cloud the tags belong to in order to obtain or update the relevant item information.

It is recommended that the physical digital twin tag contains data indicating within which cloud its associated data resides. It is recommended that a standard method is used; GS1 provides such service for electronic product codes (EPCs). Annex B.4 shows how ISO/IEC 20248 can be used to construct a digital twin tag within a self-managed method.

2.2. Identification tags

An identification tag is a tag which uses a well-known (standard and self-managed) numbering method from which the object identity and issuer/owner can be inferred, e.g. the GS1 EPC identifies a unique object (e.g., product, asset, logistic unit) or location, an IATA tag can be identified as representing in transit baggage and an ISO/IEC 20248 structure points to an X.509 digital certificate which specifies the owner of the tag and the data it contains.

It is similar in nature to a digital twin tag however the well-known (standard specified) number is useful to a local (Fog and Edge) system; this is beneficial, especially when a cloud service is not reliably or determinately available. Often the number contains information about the object, e.g. a baggage tag number also contains the Julian flight date. An EPC SGTIN mates a Global Trade Item Number (GTIN) with a serial number, uniquely identifying an instance of a product / trade item. A well-known ISO/IEC 20248 vehicle identification number contains the licence plate number and the visual parameters of the vehicle as described by a digital certificate issued by the government, e.g. Kenya and the Philippines. This means that tag data can be federated between independent systems/services without the need to connect independent data bases, as such reducing the operational and security burdens of interconnected data bases.

Additional information is, however, still required to decode and interpret the identification number. This information needs to be acquired, at least once, from a trusted source; a standard specification, a data structure register or in the case of ISO/IEC 20248, the relevant digital certificate.

2.3. Information tags

An information tag contains additional data about the object to which it is attached. This information may be static data such as an expiry date for a pharmaceutical product or it can be dynamic data such as that from a temperature sensor. Some toll systems write the road entry time and place to a vehicle's tag to determine the associated cost when the toll road is exited. Other examples include tags associated to machinery which may record the service dates and asset tags that may contain owner, sub-owner, and usernames.

In all these cases, the information is immediately available from the tag allowing local decision making and actions; however, this requires more tag memory and more time to access the tag memory. External information to decode and interpret the data received from the tag may be needed.

3. Reading RAIN tags

Providing systems that are capable of dealing with RAIN flooding and acid RAIN would appear to be daunting, but these issues can be overcome by following the principle of the RAIN Reader Communication Interface (RCI) Guide. Generally, a system knows which type of tags it expects to be read in a specific read zone. It also knows what other data it needs from the tag and how to access the data.

The RAIN RCI is specifically developed to allow readers to be optimised for a specific purpose, whilst remaining interoperable with other readers. For example, a vehicle toll point is only interested in toll tags, a baggage handler is only interested in a baggage tag, and a shop is only interested in EPC SGTIN tags; each with their own read scenario parameters. The reader may therefore ignore all the other tags in the read zone and limit itself to the information the targeted tags provide. However, as well as the intended toll tags, current tolling systems commonly also often identify vehicle parts tags applied during the manufacture of the vehicle and can therefore safely be ignored. One way of efficiently achieving this is for the toll system to use the RAIN RCI to instruct the reader to filter out the irrelevant tags. Through this mechanism these unwanted tags are not even reported to the toll systems. Such an RCI instruction is contained in a tag access schema called a spot profile.

Both the RAIN Reader Communications Interface (RCI) Guide and GS1 Low-Level Reader Protocol (LLRP) provides a standard method to filter tags to deal with RAIN flooding and acid RAIN, provided the numbering recommendations are followed.

It is often the case that developers of closed and proprietary systems believe only their tags will appear in their system's read zones. RAIN Alliance presentations and discussions in 2019 including a dedicated *RAIN flooding and acid RAIN* presentation contested this. RAIN members have reported interference by other tags, and they acknowledge that their tags may interfere with other systems.

The RAIN RCI provides methods for proper programming of RAIN tags and interpretation of specified RAIN data. All RAIN read events are reported in the de facto Internet data message format JSON (ISO/IEC 21778) using field names and field values. This allows both humans and machines to easily understand and use the information on a tag. RCI reports are designed to be reported on a standard serial data channel like USB and TCP/IP or a messaging transport protocol such as MQTT (ISO/IEC 20922). MQTT is a favourite technology used as the engine for IoT middleware operating on the Edge and in the Fog.

The GS1 LLRP provides fine-grain control of the RAIN air protocol allowing RAIN-"intelligent" applications to deal with the issues as reported in this technical note. LLRP is designed to connect to the GS1 full-service data stack and cloud services.

4. RAIN tag data components

Thought should go into the information that is required to be encoded on a tag. A high-level technical understanding (especially for business leaders and solutions architects) of the tag data components will avoid problems later.

The physical composition of the tag memory is provided in Annex A. A RAIN tag contains the following data elements:

1. A compulsory object identifier, stored in MB 01 (UII/EPC), which is obtained during inventory of the tags. This is the first step in accessing the tag data.

   The object identifier may be a simple number to a unique "fingerprint" consisting of more than one field, of the objects often using alphanumeric values and even formatted references like a map-point.

   This identifier uniquely identifies the tagged object. This identifier may be linked (in databases) to supplementary information (or "master data") about the object, such as shape, colour, and dimensions of a product, vehicle, or container. ISO standards call this unique identifier the Unique Item Identifier (UII), while GS1 calls it the Electronic Product Code (EPC), normatively specified in the GS1 EPC Tag Data Standard (TDS).

   The so-called "Toggle" (or "T") bit 17_h of MB 01 indicates the identification system encoded, either:

   (0) an EPC (GS1) application, with a binary encoded EPC beginning at bit 20_h;

or

(1) an ISO Application Family Identifier (AFI) at bits 18_h-$1F_h$, followed by a Unique Item Identifier (UII) appropriate for the encoded AFI.

The Toggle bit is backscattered with the other Protocol Control (PC) bits during inventory of a tag's UII/EPC.

2. A compulsory unique tag identifier, the TID, which at a minimum indicates make and model of the chip. It is written, and permalocked, to MB 10 (TID) by the chip manufacturer. An extended TID (XTID) may contain optional chip serialisation and additional information about the capabilities of the tag (e.g., supported command set).
3. Optional, supplementary information about the tagged object:
   a. Additional information about the tagged object may be stored in the tag's User Memory, MB 11.
   b. Tag use information is a set of flags contained in the extended Protocol Control (XPC) bits which is sent by the tag with the UII/EPC during inventory of the tags. XPC is stored in MB-01 and obtained during inventory.
4. Optional sensor data:
   a. Snapshot sensor and simple sensor data are contained in the extended Protocol Control (XPC) bits, which are backscattered by the tag along with the UII/EPC during an inventory operation. This sensor data is specified in ISO/IEC 18000-63 with a clear and well-known interpretation (and optionally interpreted by RCI from Version 4).
   b. Complex sensor data must be additionally read after access to the tag is gained (ISO/IEC 24753). This sensor data requires additional information to decode and interpret it. It allows for the addition of new sensors at any time.
5. Optional tag access data provides control over access to the tag data:
   a. Kill and access passwords, stored in MB 00 (Reserved memory):
      i. The access password allows a reader to read and write data in access operations from/to a tag which has been closed for general access. The default state for a tag is to be open for general access.
      ii. The kill password allows the reader to kill a killable tag. The default state for a tag is not to be killable.
   b. Crypto suites, where the tag and the reader communicate over an encrypted channel, ensures access to data on the tag is limited to holders of the relevant crypto key(s). The encrypted data channel ensures that data sent over the air appears to be scrambled continuously, preventing eavesdropping, tag data insertion and tag traceability by non-authorised readers.

Note, passwords are sent in clear over the air and can be eavesdropped. Keys are never sent over the air.

5. Tag data security

Tag data security can be divided into the following outcomes:

1. Tag data access control whereby only an authorised reader is allowed to access the protected data on the tag. Tag access enables tag data privacy and prevents the changing of protected information on the tag. It can also prevent tracking of tags by eavesdroppers.
2. Tag data integrity verification whereby the integrity of the data and its source (the entity that encoded the tag data) can be verified by an application or a reader.
3. Tag copy detection whereby an application or a reader can detect that the tag is fake.
4. Tag replay detection whereby an application or a reader can detect that the tag read instance (a spot) is fake.

A combination of security functions will provide optimal protection in terms of risk, cost, and performance. It is important to note that an increase in tag data security will result in reduced read performance (range and speed) and will also increase the cost of the tag, the reader, and the data infrastructure. ISO/IEC 21227 provides measurement methods to determine the impact of on-chip crypto on the performance of the tag.

Tag security methods are discussed in detail in the RAIN whitepaper *Privacy and Security Considerations in RAIN RFID Systems*.

5.1. Tag data access

RAIN tags may support the following tag data access models (access methods may apply to the whole tag or parts of the tag memory):

1. Open: The tag data can be accessed by all readers.
2. Read-only: The data can be read by all readers, but not written or changed.
3. Private data:
    a. The data stored on the tag can only be accessed using the access password. This applies independently for reading and writing.
    b. The data is stored on the tag is in an encrypted state (ISO/IEC 20248). This data is read and forwarded to an application in its encrypted form. Only applications with the key can decrypt and interpret this data. Both symmetric and asymmetric encryption methods can be used. Encrypted data is commonly larger than its unencrypted form, as such, encrypted data requires more tag memory and time to access.
    c. The data is encrypted by the tag before it is transmitted to the reader (ISO/IEC 29167).
        i. Only readers and applications with the correct key can decrypt and use the data.
        ii. The on-chip crypto may be used to authenticate the reader before a tag will communicate with it.
4. Untraceable data: The tag data is accessed in a manner that will limit the ability to track the tag by eavesdropping the communication between reader and tag. Untraceability is achieved through one or more of the following methods:
    a. Tag reduction of its read range.
    b. Make the tag and object identifying data (the unique parts of the data) private. Tags remain identifiable in groups, but not individually, which allows the reader to select the right key/password to access the private parts.

c. Scramble the data sent over the air by using on-chip crypto.

   The encryption includes a random challenge from the reader ensuring that the data transmitted appears to be random to an eavesdropper.

   Note, this may be problematic since the reader/application must know which key to use, which in conflict, requires some identification information from the tag that makes it traceable. This means that on-chip crypto enabled untraceability is only feasible where large groups of tags share the same key. Even key-diversification is a victim of this conflict.

5. No access: Access to tag data can be permanently removed by killing the tag. All tags can be killed by physical destruction (a hammer works well ☐). A more elegant way is for a reader to instruct the tag, with a kill password, to die permanently.

   "To kill, or not to kill, a tag?" is an important question!

   a. A tag should be killed after it performed its duty representing an object when the tag data may be used to infringe an individual's privacy. For example, the purchase habits of a person could potentially be revealed through tag data.
   b. Data on a retired tag or a group of retired tags may reveal confidential company information, in which case the tags should be killed. For example, disposed tags can be read when the rubbish is collected and reveal the brand, type and volume of consumables used by a hospital.
   c. If the kill command is supported, password management procedures must be vetted and in place prior to deployment. Given the risk posed by a single, harmonised password for one entire class of a tagged object (i.e., in the retail environment, for ALL serialised instances of a given GTIN), serious consideration should be given to a unique password for each individual tagged object. This pertains not only to password allocation but also communication of passwords to downstream parties whose identity might not be known at the time of source tagging.

Note, these examples are overstated (hyperbole) to illustrate reasons to kill tags. The RCI and LLRP provides an efficient way to kill retired tags. Some readers are optimised to be dedicated very efficient tag killing machines.

5.2. Tag data integrity protection:

Integrity protection of data is the ability to verify the identity of the issuer of the tag data and to detect that tag data has not been altered. This is achieved using any combination of the following methods:

1. Chip level protection uses on-chip crypto (ISO/IEC 29167): the tag and the reader share a secret key. This key is typically issued and managed by the tag data issuer. Integrity of the data is based on the secrecy of the key which is only distributed to trusted parties. The trusted parties have confidence that, assuming the data decrypts correctly when using the appropriate key, that the data was programmed originally by the appointed tag issuer and that it has not been tampered with since.

   Note, all current market available ISO/IEC 29167 methods use symmetric keys. The same key is used to encrypt and decrypt; therefore, entities that can verify current ISO/IEC 29167 tag data can also create new tag data with the same key. Key management is

therefore critical and shared keys and passwords should be protected with cyber security methods and hardware crypto vaults available. Unfortunately, there is no current standard key management method for ISO/IEC 29167. ISO/IEC 20248 may be used to enable key management for ISO/IEC 29167.

Chip level crypto provides an effective method against over-the-air eavesdropping. This can be used to provide tag data privacy protection and untraceability for groups of tags.

2. Data level protection (ISO/IEC 20248) uses asymmetric encryption and X.509 PKI which is the security of the Internet (digital signatures and certificates). Asymmetric encryption uses two keys. The one is used to encrypt the data; this is the private key. The other is used to decrypt the data; this is the public key. The data issuer keeps the private key secret and uses it to encrypt (sign) the tag data. A trusted third party uses a X.509 digital certificate to publish the public key and certifies the owner of the public key. If the data decrypts correctly (using the public key), then only the data issuer could have encrypted it and the data was not tampered with, i.e. data source and data integrity verification.

   Note, a digital signature does not provide privacy of data since the public key is not required to be secret. It also does not provide for untraceability. The public key cannot be used to create or tamper with tag data.

   Asymmetric encryption and X.509 are the backbones of all digital security. You trust it every day with your money, business, and personal information. Asymmetric-key management is well sorted and inherently part of the data, data structure and data owner verification as practiced in the Internet.

   ISO/IEC 20248 provides the most effective and efficient method for tag data integrity for RAIN tags to barcodes.

5.3. Tag copy detection

The object identifier (UII/EPC) is programmable on all current RAIN tags. Many systems rely on the assumption that these identifiers are not merely copied from one tag to another, i.e. no tag duplicates exist in the system, which is sadly not always true. The occurrence of duplicates, both accidental and malicious, have been reported in many applications. Duplicate tags not only confuse systems but can be used to access information referenced by the identifier as with digital twin tags, or could potentially result in a denial-of-services attack.

Tags require an unchangeable unique component to make copied tags detectable. The TID, by convention, is burned in (written once and locked), by the chip manufacturers; XTID allows for optional inclusion of a chip's serial number.

A local application could use the TID of a digital twin tag to obtain the associated object information from the cloud. However, this does not prevent a rogue application soliciting information from cloud storage. TID serialisation could unintentionally assist in unauthorised mining of cloud data. Chip level crypto provides an effective method for a cloud service to detect information solicitation.

Chip level crypto and digital signatures are also effective measures to detect identification and information tag copies.

5.4. Tag replay prevention

"Ghost" tag reads can be manufactured by replaying a recorded tag reader conversation. Objects may therefore be recorded to be at a certain place without actually being there. Untraceability is an effective tag function to prevent and detect such replays. On-chip crypto is especially effective for this function.

Rough readers may also report tag reads which did not actually take place. Protecting against rough readers and applications requires Cyber Security measures. The standards world provides excellent guides and methods, for example X.509 and SSL/TLS which are commonly used in the Internet and by LLRP. ISO/IEC 20922 MQTT is a messaging bus for sensors which supports X.509 and SSL/TLS. The RAIN RCI is designed to use MQTT as a messaging bus.

Bibliography

RAIN Memphis presentation *RAIN flooding and acid RAIN*.

RAIN Florence presentation *TagFlooding_RaceResult_Florence_2019*.

RAIN guide *RAIN Reader Communication Interface (RCI).*

RAIN whitepaper *Privacy and Security Considerations in RAIN RFID Systems*.

GS1 *EPC Tag Data Standard (TDS).*

GS1 *Low Level Reader Protocol (LLRP).*

ISO 17367 *Supply chain applications of RFID — Product tagging*

ISO/IEC 15961 all parts *Information technology — Data protocol for radio frequency identification (RFID) for item management*.

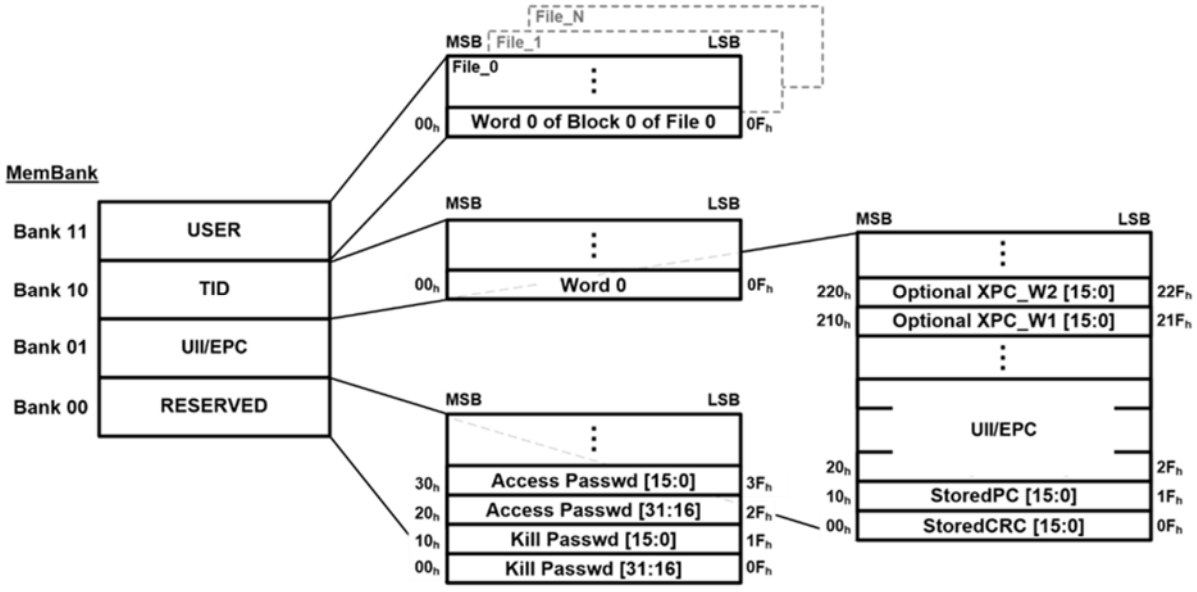
ISO/IEC 20248 *Automatic Identification and Data Capture Techniques — Data Structures — Digital Signature Meta Structure*.

ISO/IEC 21227 *Information technology — Radio frequency identification device performance test methods — Crypto suite*

Annex A RAIN tag memory map

The following RAIN tag memory map indicates the logical location of the tag data components. A RAIN tag contains 2 to 4 memory banks:

0. MB 00: Optional - This memory bank is reserved. Chip specific data like passwords and keys are stored here. This memory bank is not generally accessible by readers in the field.
1. MB 01: Compulsory - This memory bank is transmitted to the reader during the tag inventory process. It contains:
    a. The object identifier (UII/EPC).
    b. The protocol control (PC and -- optionally -- XPC) bits which include, but are not limited to:
        i. The number system toggle between EPC/GS1 (0) and ISO (1)
        ii. Optional tag use flags
        iii. Sensor data.
2. MB 10: Compulsory - The tag identifier (TID), optionally extensible (XTID) to include chip serialisation and support for protocol command sets.
3. MB 11: Optional - User memory. Additional information about the tagged object may be stored in this memory bank. Sensors may be memory mapped into this memory bank.



Annex B Encoding details

This annex discusses tag encoding details and tag data reporting at the hand of the RAIN Reader Communication Interface (RCI) Version 3.

A RAIN tag contains:

- An object identifier (UII/EPC) typically programmed by the object owner into MB01. MB01 also contains the PC word and optional XPC words (XPC_W1 and XPC_W2), which is reported by the tag, during INVENTORY, before the UII/EPC.
- A tag identifier (TID) serialised (XTID), programmed, and locked by the chip manufacturer.
- Optional object information, tag use and access information.

Many commercial RAIN readers do not report the PC word. In this case, an application cannot detect if a tag has ISO or GS1 data. Also, XPC words are often erroneously reported as part of the "EPC" resulting in the application receiving an incorrect UII/EPC. See Annex C for the correct reporting of PC and XPC words.

The correct way for a reader to report RAIN tag data is as follows:

MB-01 PC	MB-01 XPC	MB-01 UII/EPC	MB-10 TID	MB-11 User Memory
16 bits	X * 16 bits	Y * 16 bits	96 bits	X * 16 bits

X = 0, 1 or 2.
Y = 0 to 31

The PC word has the following information:

MB-01 PC Word				
UII/EPC length	UMI	XI	Standard (T bit)	ISO:AFI GS1: RFU
5 bits	1 bit	1 bit	1➔ISO & 0➔GS1	8 bits

The T bit indicates ISO or GS1 tag data.
The AFI indicates the type of ISO data.
UMI indicates that user memory is available.
XI indicates that XPC is included in the inventory.

The RAIN Reader Communication Interface (RCI) reports tags as ISO or GS1 (UII or EPC) as follows:

ISO: T=1

```
{"Report":"TagEvent","AFI":":92","UII":":0123:4567:89AB:CDEF"}

{"Report":"TagEvent","AFI":":00","UII-NOT-CONFIGURED":":0123:456…"}
```

For AFI=0x01 to 0x07

```
{"Report":"TagEvent","AFI":":03","UII-PROPRIETARY":":0123:4567…"}
```

GS1 T=0 GS1's EPC Tag Data Standard (TDS) specifies the EPC scheme using the EPC header value.

Header=0x00

```
{"Report":"TagEvent","Scheme":"UNPROGRAMMED","EPC":":0022:1234…"}
```

Header=0x2C to 0x41

```
{"Report":"TagEvent","Scheme":"SGTIN","EPC":":3003:4567:89AB…"}
```

Header 0xE0 and 0xE2

```
{"Report":"TagEvent","Scheme":"TID","EPC":":E203:4567:ABCD…"}
```

The TID EPC Scheme is specified in GS1's EPC Tag Data Standard (TDS).

TID is PERMANENTLY RESERVED to avoid confusion with the first eight bits of TID memory when the TID has been copied to UII/EPC. Many chips are shipped with the TID copied to the UII/EPC.

All other header values shall be reported as RFU (reserved for future use).

```
{"Report":"TagEvent","ErrID":0,"Scheme":"RFU","EPC":":0103:4567:89AB…"}
```

RCI reports XPC and user memory as illustrated in the following example:

```
{"Report":"TagEvent","DT":"2017 09 11T13:06:01.000",
 "Spot":"Seen","InvCnt":25,"PC":":3592:0025",
 "AFI":":01","UII-PROPRIETARY":":0123:4567:89AB:CDEF:89AB:CDEF",
 "MB":[{"ID":3,"Start":0,"Data":":2323:2323:2323:2323"}]}
```

B.1 Standard-managed object number schemes (Identification tags)

B.1.1 ISO tag data

ISO object number schemes (unique item identifier - UII) are specified by registered organisations, like IATA, who is assigned an ISO/IEC 15961 AFI by the ISO Registration Authority AIM Inc., see https://www.aimglobal.org/registration-authority.html.

ISO/IEC 15961 also specifies a set "reserved" AFIs for closed applications.

- AFI 0 indicates that the tag is not configured.
- AFIs 1 to 3 may be used for proprietary tag data.
- AFIs 4 to 15 is assigned to special closed applications.

When ISO tag data is used, then the Standard Toggle (T) bit shall be set to 1. Typically, a Data Structure Format (DSFID) is defined for the UII. An example an IATA bag tag, as specified by IATA RP1740C, is illustrated below.

MB-01 PC Word					MB-01 UII/EPC		
UII length	UMI	XI	Standard	AFI	UII as specified by IATA RP1740C		
					DSFID	Baggage ID number	Julian Flight Date
00110	0	0	T=1 (ISO)	0xC1	0x0C	0x21050123456789	0x1202015E

The following RCI Spot Profile is used to instruct a reader to only read and report IATA bag tags once:

```
{"Cmd":"AddProf","EncodingType":":C1"}
```

The above example will be reported as follows:

```
{"Report":"TagEvent","AFI":":C1","UII":":0C21:0501:2345:6789:1202:015E"}
```

The following RCI Spot Profile is used to instruct a reader to program the next tag in the read zone with the example IATA bag tag data (the write will be checked, and the tag locked):

```
{"Cmd":"AddProf","DwnCnt":1,"WriteUII":[":2105:0123:4567:8912:0201:5E",[":C1","
:0C"],true,"SECURED"]}
```

Note, the DSFID (0x0C) is added to the front of the UII. The DSFID will not be prepended when not specified. As such the following Spot Profile will have the same result.

```
{"Cmd":"AddProf","DwnCnt":1,"WriteUII":[":0C21:0501:2345:6789:1202:015E",[":C1"
],true,"SECURED"]}
```

B.1.2 GS1 tag data

The widely adopted Electronic Product Code (EPC) encodings are standardised and maintained by GS1 and **specified in detail in the GS1 EPC Tag Data Standard (TDS).**

The following example illustrates an SGTIN-96 encoding:

MB-01 PC Word					MB-01 UII/EPC	
EPC length	UMI	XI	Standard	RFU	EPC as specified by GS1 TDS	
					Header	Company, Item Reference & Serial
00110	0	0	T=0 (GS1)	0x00	0x30	0x00050123456789 1202015E

The following RCI Spot Profile is used to instruct a reader to only read and report an SGTIN tag once:

```
{"Cmd":"AddProf","EncodingType":"SGTIN"}
```

The above example will be reported as follows:

```
{"Report":"TagEvent","Scheme":"SGTIN","EPC":":3000:0501:2345:6789:1202:015E"}
```

The following RCI Spot Profile is used to instruct a reader to program the next tag in the read zone with the example SGTIN tag data (the write will be checked, and the tag locked):

```
{"Cmd":"AddProf","DwnCnt":1,"WriteEPC":[":3000:0501:2345:6789:1202:015E",true,"
SECURED"]}
```

Note, the EPC header is included in the EPC to facilitate a direct link with the GS1 data stack.

B.1.3 Standard based information tags

Tag use and sensor information is delivered through the XPC bits, in which case the XI bit in the PC bits will be set. RCI will then deliver all the XPC bits as part of the report. Future versions of RCI will provide sensor data interpretation as specified by ISO/IEC 18000-63 and ISO/IEC 24753.

GS1 and ISO specifies (ISO/IEC 15961) that object information shall be stored in User Memory MB-11. The first 8 bits of MB-11 shall contain the DSFID.

MB-01 PC Word					MB-01 UII	MB-11 User Memory	
UII/EPC length	UMI	XI	Standard	AFI/RFU	UII/EPC	DSFID	Data fields according to ISO/IEC 15961 & 15962
5 bits	1	0	1➔ISO & 0➔GS1	8 bits	X * 16 bits	8 bits	≥ 0 bits

The following command will program, verify, and lock both an UII and User memory:

```
{"Cmd":"AddProf","DwnCnt":1,"WriteUII":[":2105:0123:4567:8912:0201:5E",[":C1","
:0C"],true,"SECURED"],


"WriteUM":[":AAAA:BBBB:CCCC:DDDD",":00",true,"SECURED"]}
```

DSFID 0 means there is no format and DSFID 30 means the format is proprietary.

The following Spot Profile will read and report the above example:

```
{"Cmd":"AddProf","EncodingType":":C1","Read":[[3,0,5]]}
```

It is important to note that a DSFID may specify a data format which is limited to an encoding type, or it may specify a data structure method. For example:

- **Registered** data schemes: DSFID 1 (0x01) indicates the format of the User Memory data is packed objects using the ISO/IEC 9834-1 registered data objects.

MB-01 PC Word					MB-01 UII	MB-11 User Memory	
UII/EPC length	UMI	XI	Standard	AFI/RFU	UII/EPC	DSFID	ISO/IEC 9834-1 packed object data
5 bits	1	0	1➔ISO & 0➔GS1	8 bits	X * 16 bits	0x01	≥ 0 bits

- **Self-managed** data schemes: DSFID 17 (0x11) indicates the format of the User Memory data according to ISO/IEC 20248.

MB-01 PC Word					MB-01 UII	MB-11 User Memory			
UII/EPC length	UMI	XI	Standard	AFI/RFU	UII/EPC	DSFID	DAID	CID	ISO/IEC 20248 data
5 bits	1	0	1➔ISO & 0➔GS1	8 bits	X * 16 bits	0x11	32, 40 or 48 bits	16 bits	≥ 0 bits

B.2 Self-managed tag data (Identification and Information tags)

ISO/IEC 20248, which can work with any identification scheme, specifies a method whereby data stored within a barcode and/or RFID tag are structured, encoded and digitally signed. ISO/IEC 15459 registered companies and organisations can develop and manage their own object numbers and tag data, see https://www.aimglobal.org/registration-authority.html. AIM Inc. registers Issuing Agencies who in turn issue Company Identification Numbers (CINs). For example, the Euro Data Council (http://www.eurodatacouncil.org/en/) has the IAC="QC". The GS1 Global Office is assigned the Issuing Agency Codes (IACs) "0" to "9". The Euro Data Council assign 4-letter CINs and GS1 a decimal number CIN.

ISO/IEC 20248 calls the registered companies and organisations the domain authority (data owner) who is identified with the DAID which is constructed from the IAC and CIN. For example, the Euro

Data Council assigned the 20248.org demo system the CIN "DGSG". The DAID for 20248.org is therefore "QC DGSG" which will encode into 40 bits, 0xC098099640.

ISO/IEC 20248 is assigned the AFI 0x92. Native ISO/IEC 20248 tag data is depicted below. An ISO/IEC 20248 data structure may span all the RAIN tag memory banks; the UII/EPC, MB-01 memory not assigned to the UII/EPC, MB 10 TID and MB-11 User Memory. It does not use a DSFID since it specifies its own format.

MB-01 PC Word					MB-01 UII/EPC extendable to included MB-10 TID and MB-11 User Memory		
UII length	UMI	XI	Standard	AFI	UII as specified by ISO/IEC 20248		
					DAID	CID	Self managed item number and information
5 bits	0	0	T=1 (ISO)	0x92	32, 40 or 48 bits	16 bits	X * 16 bits

The CID is an identifier for the data structure description contained in a X.509 digital certificate allowing for ~65,000 data structures per DAID. A CID may be reused once the reference to which it points expires.

The following RCI Spot Profile is used to instruct a reader to program the next tag in the read zone with the ISO/IEC 20248 data (the write will be checked and the tag locked; note ISO/IEC 20248 does not use an DSFID in the UII):

```
{"Cmd":"AddProf","DwnCnt":1,"WriteUII":[":C098:0996:4005:2345:6789:1202",[":92"
],true,"SECURED"]}
```

The following RCI Spot Profile is used to instruct a reader to only read and report ISO/IEC 20248 tags once:

```
{"Cmd":"AddProf","EncodingType":":92"}
```

The RCI Spot Profile can be refined only to read a specific companies tags, say "QC DGSG" as follows:

```
{"Cmd":"AddProf","EncodingType":":92","MBMask":[1,32,40,":FFFF:FFFF:FF",":C098:
0996:40"]}
```

The above example will be reported as follows:

```
{"Report":"TagEvent","AFI":":92","UII":":C098:0996:4005:2345:6789:1202"}
```

RCI has the ability to interpret tag data. Version 3 caters for ISO/IEC 20248. Later versions will include data interpretation of appropriate tag data methods, like GS1 TDS and sensor data. Following is an example of RCI interpreted ISO/IEC 20248 tag data; note, the DAID, CID and fields. This example also contains a digital signature stored in MB-11 and the TID which is used to detect data tamper and tag copies. The digital signature and TID is shown in Base64 binary representation. The second timestamp indicates when the data was written to the tag.

```
{"Report":"TagEvent","TimeStamp":1571795244.815,

 "AFI":":92","UII":":C098:0B4F:7500:6B00:799A:3186:4714:1000",

 "20248":{"ResponseCode":{"Code":5,"Desc":"DigSig Verification accepted; No
error"},

          "DDDdataTagged":{"specificationversion":"ISO/IEC
20248:2018","timestamp":1511246331,
```

```
                                "daid":"QC
FVXX","cid":107,"dauri":"https://da.fleetvalid.info",

                                "license_plate":"QCOP75","plate_placing":"FRONT",

                                "vehicle_colour":"WHITE","vehicle_shape":"SEDAN",

                                "signature":"BSeYOt9ajay_RrTKYIOKN6Uz-
9txxKXFQMambkWAKi4=",

                                "tid":"4sBokiAAMAAePDZn"}}}
```

B.3 Proprietary tag data (Identification and Information tags)

Proprietary tag data may cause acid RAIN. The use of it should be avoided as far as possible. Note, in the following examples proprietary tag data will not interfere with standard data but may interfere with other proprietary tag data systems.

The EPC header 0x00 indicates an Unprogrammed Tag, with the toggle bit de-asserted (i.e, set to 0), **in violation of GS EPC TDS:**

MB-01 PC Word					MB-01 UII/EPC	
EPC length	UMI	XI	Standard	RFU	EPC header	Proprietary tag data
5 bits	0	0	T=0 (GS1)	0x00	0x00	0x12345678…

RCI will report this tag as follows:

```
{"Report":"TagEvent","Scheme":"UNPROGRAMMED","EPC":":0012:3456:78…"}
```

It is programmed with:

```
{"Cmd":"AddProf","DwnCnt":1,"WriteEPC":[":0012:3456:78…",true,"SECURED"]}
```

The proper proprietary method is to use ISO tag (T=1) data with the AFI set to a value 1 to 3.

MB-01 PC Word					MB-01 UII/EPC extendable to included MB-10 TID and MB-11 User Memory
UII length	UMI	XI	Standard	AFI	Proprietary data
5 bits	0	0	T=1 (ISO)	0x01	0x01234567

RCI will report this tag as follows:

```
{"Report":"TagEvent","AFI":":01","UII-PROPRIETARY":":0123:4567…"}
```

It is programmed with (the default AFI in RCI is 1):

```
{"Cmd":"AddProf","DwnCnt":1,"WriteUII":[":0012:3456:78…",true,"SECURED"]}
```

AFI 0 will be reported by RCI as follows:

```
{"Report":"TagEvent","AFI":":00","UII-NOT-CONFIGURED":0123:456…"}
```

B.4 Digital twin tags

A digital twin tag references a record in a cloud. A value in the UII/EPC memory can be used though these values may be easily copied to another tag and go undetected. Also, in this way there is no standard method to determine which cloud to use.

A standard based digital twin tag can be constructed using the TID (the serialisation part) and ISO/IEC 20248 DAID.

MB-01 PC Word					MB-01 UII	MB-10 TID	
UII/EPC length	UMI	XI	Standard	AFI	DAID	Manufacturers information	TID serialisation
00010	0	0	T=1 (ISO)	0x92	32 bits	16 bits	48 bits

The DAID points to the cloud, since the DAID is a registered company/organisation with a well-known website. The reference cannot be tampered with since it is programmed and locked by the chip manufacturer. The serialisation may be made random to prevent illegal cloud mining.

The following RCI Spot Profile reads the above digital twin tag:

```
{"Cmd":"AddProf","EncodingType":":92","Read":[[2,3,3,3]]}
```

And the report will look like this (the example DAID 0xC0980B4F is "QC FVXX" ➔ www.fleetvalid.info)

```
{"Report":"TagEvent","AFI":":92","UII":":C098:0B4F",


"MB":[{"ID":2,"Start":3,"Data":":2323:2323:2323"}]}
```

Untraceability can be achieved by providing access control over the TID. This can be done with a password or crypto key linked to the DAID group of tags. An RCI access password will look like this:

```
{"Cmd":"AddProf","EncodingType":":92","Read":[[2,3,3,3]],"AccessPWD":[":xxxx:xx
xx"]}
```

Annex C Proper reporting of the PC and XPC words

The RAIN air protocol specifications (ISO/IEC 18000-63 and GS1 EPC Gen2) specify the following:

1. The XPC words are optional for tags. The optional XPC words are stored in MB01 address from bit 210_h, see Annex A.
2. During inventory the tag shall backscatter/send the PC word, then the optional XPC words and then the UII/EPC.
3. The reader shall be able to receive and report the PC and XPC words correctly.

Readers which do not comply with the RAIN air protocol specifications typically report the XPC word(s) prepended to the UII/EPC, causing application confusion. Let us consider the following three GS1 tags:

1. With only the PC word, i.e. a standard "EPC tag":

MB01 PC Word					MB01 UII/EPC
EPC len	UserMem	XI	Standard	RFU	EPC
00110	0	0	0 (GS1)	0x00	0x301234567901234567890 12

RCI report:
{"Report":"TagEvent","PC":":3000","Scheme":"SGTIN","EPC":":3012:3456:7890:1234:5678:9012"}

A non-compliant reader reports the tag inventory correctly, but often omits the PC word resulting in the inability to detect if this is a genuine GS1 EPC tag (note, the AFI = 0x00 and as such may be an GS1 tag or a not-configured ISO tag):

PC = 0x3000 and EPC = 0x301234567901234567890 12

2. With the PC word flag XI=1; the tag also transmits XPC_W1 during inventory (note, the transmitted EPC len is incremented by 1; transmitted EPC len=00111):

MB01 PC Word					MB01 UII/EPC	MB01 XPC Word 1
EPC len	UserMem	XI	Standard	RFU	EPC	XPC_W1
00110	0	1	0 (GS1)	0x00	0x301234567901234567890 12	0x0800

RCI report:
{"Report":"TagEvent",**"PC":":3A00:0800"**,"Scheme":"SGTIN","EPC":":3012:3456:7890:1234:5678:9012"}

A non-compliant reader typically reports the tag inventory incorrectly with the XPC part of the EPC:

PC = 0x**3A00** and EPC = 0x**0800**301234567901234567890 12

The correct report is:

PC = 0x**3A00**, XPC_W1 = 0x**0800** and EPC = 0x301234567901234567890 12, or

PC = 0x**3A000800** and EPC = 0x3012345679012345678901 2.

Note, XPC_W1 is prepended to the EPC which results in the wrong EPC. This problem is worsened when the PC word is not reported. With the PC word reported, the application can detect the error.

3. With the PC word flag XI=1 and the XPC word flag XEB=1; the tag also transmits XPC_W1 and XPC_W2 during inventory (note, the transmitted EPC len is incremented by 2; transmitted EPC len=01000):

MB01 PC Word					MB01 UII/EPC	MB01 XPC Word 1	MB01 XPC Word 2
EPC len	UserMem	XI	Standard	RFU	EPC	XPC_W1	XPC_W2
00110	0	1	0 (GS1)	0x00	0x3012345679012345678901 2	0x8100	0x2222

RCI report:
{"Report":"TagEvent","**PC":":4200:8100:2222**","Scheme":"SGTIN","EPC":":3012:3456:7890:1234:5678:…"}

A non-compliant reader typically reports the tag inventory incorrectly with the XPC part of the EPC:

PC = 0x**4200** and EPC = 0x**81002222**3012345679012345678901 2

The correct report is:

PC = 0x**3A00**, XPC_W1 = 0x**8100**, XPC_W1 = 0x**2222** and EPC = 0x3012345679012…9012, or

PC = 0x**3A0081002222** and EPC = 0x3012345679012345678901 2.

Note, XPC_W1 and XPC_W2 are prepended to the EPC which results in the wrong EPC.

ABOUT RAIN RFID ALLIANCE

The RAIN RFID Alliance is an organization supporting the universal adoption of RAIN UHF RFID technology. A wireless technology that connects billions of everyday items to the internet, enabling businesses and consumers to identify, locate, authenticate and engage each item. The technology is based on the EPC Gen2 UHF RFID specification, incorporated into the ISO/IEC 18000-63 standard. For more information, visit www.RAINRFID.org. The RAIN Alliance is part of AIM, Inc. AIM is the trusted worldwide industry association for the automatic identification industry, providing unbiased information, educational resources and standards for nearly half a century.

RAIN RFID Alliance

One Landmark North
20399 Route 19
Cranberry Township, PA 16066

Visit the RAIN RFID website – RAINRFID.org. If you are interested in learning more about the RAIN RFID Alliance, contact us at info@rainrfid.org.