RAIN flooding and acid RAIN

RAIN Memphis – March 2019

Bertus Pretorius – apretorius@licensys.com

The humongous success of RAIN may result in two negative outcomes;

and we are starting to see signs of it!

We need to act now with the RAIN Alliance taking the lead.

RAIN flooding

RAIN flooding occurs when:

- To many tags are in the ReadZone and some are not read.
- Other RAIN enabled services' tags in the beam prevent the targeted tags to be read.

thefloodcompany.co.uk/flooding-in-paris/

Acid RAIN

Acid RAIN occurs when:

- Other tags appear to be targeted tags.
- Tags are cloned and manipulated to appear to be a legitimate targeted tag.
- A killed tag happens to be alive and well; a zombie!

byjus.com/chemistry/acid-rain/

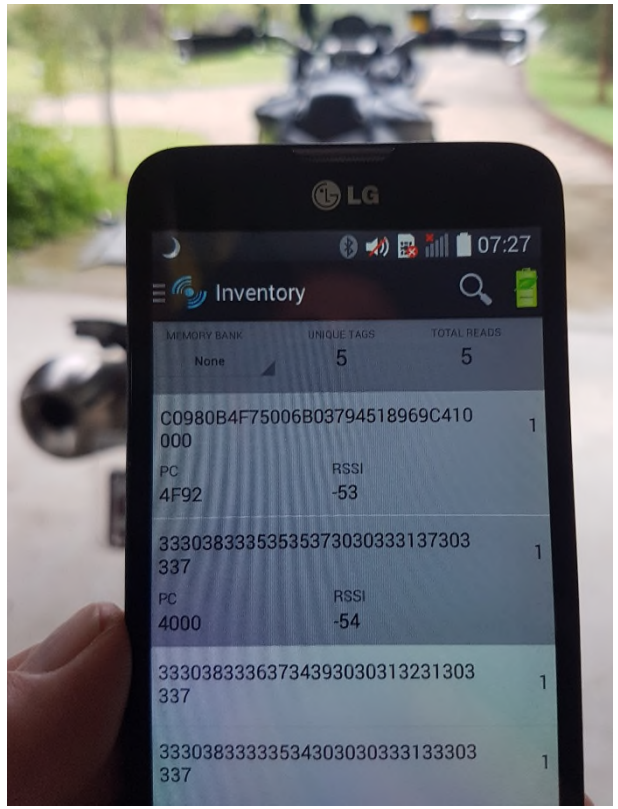
*A **targeted tag** is a tag which is targeted to be read in the ReadZone of a specific reader of an RAIN enabled service.*

Example: Electronic Vehicle Identification

In the picture the RAIN enabled number plate tag is read using a handheld reader.
The plate tag shows up
- UII: C0980B4F75006B… with PC: 4F92 indicating it is an ISO tag with an ISO/IEC 20248 data structure,

but three other tags starting with
- EPC: 33303833 with PC: 4000 indicating it is an GS1 tag, but encoded with ASCII representing "3083…".

In fact, the motorcycle has five other tags.



Example: Sport

In sport timekeeping we have two recent examples:

- Cloned tags cheating the system.
- Additional tags on runners which confused the system.

Proper data structures may allow the sharing of the tags between service providers. For instance a shoe tag may be used by different sport systems like time keeping and in the gym.

Example: Healthcare

Consider a RAIN enabled hospital.

We may find the following tags, each potentially being used by a independent RAIN service:

pharmaceuticals, consumables, machine parts, equipment, tools, assets, linen, reticulation parts, cleaning units, emergency units, documents, patients, etc.

Additionally people's items and visiting vehicles, containers, tools and equipment may also be tagged.

Clipart: RAINrfid.org and pngtree.com/freepng/cartoons-worry-sweating--scratching-the-head_3431333.html

To the RESCUE:

The RAIN Reader Communications Interface (RCI) and data standards.

Types of RAIN data

Digital Twin tags are tags which point to a record in the cloud which contains all the knowledge of the item the tag represents.

- These tags are the **smallest, cheapest and fastest to read** but the tag data only becomes useful once the cloud has been accessed. Cloud data may be cheap, **but protecting, accessing and sharing cloud data is not cheap** and may be accessible to competitors.

Identification tags are tags with a well-known (standard) schema for which the item identity and issuer/owner can be deduced, e.g. the GS1 EPC points to a company and item class and an ISO/IEC 20248 structure points to a Digital Certificate which tells you who's tag it is, how to decode it into named data and how to verify it.

- Identification for sets of tags are immediate to the local application once it acquired the external data, e.g. tags for pharmaceutical and consumable items with manufacturing and/or expiry dates.
- Attributes needs to be obtain or be predetermined.

Attribute tags are tags which contain additional information about the item. It works the same as identification tags.

- The attributes are immediately available but require more tag data and more time to read.
- GS1 TDS uses ISO/IEC 15434 packet objects with MH10.8.2 Data Identifiers and ISO uses Application Family Identifiers (AFI) which use registrar defined fields which need to be obtained every time it is updated.
- An ISO/IEC 20248 structure points to a Digital Certificate which tells you whose tag it is, all the attributes, how to decode it into named data and how to verify it.

RAIN data access

Read-only, **writeable** and **lockable** tags with a **unique TID**.

Untraceable tags are tags where the access range is reduced and/or the open data is limited to prevent the identification of individual tags. The latter may be achieved through:

- Shortening the UII/EPC which does not give anything away during INVENTORY ➔ **weak**.
- An access password where the identification and attribute data are only accessible with the use of a password ➔ **OK** and pretty **good** with the NEDAP proposal which RCI will start work on ☺.
- An crypto tag where the identification and attribute data are only accessible through the use of a crypto graphic function and a key. The air link is typically encrypted and random, but this takes more time and reduces the read range ➔ **strong**.

Verifiable tags are tags where the tag and the tag data is verified using any combinations of:

- Access password – the data is not verifiable once the tag is gone ➔ **OK**.
- Crypto ➔ **strong** and with the RCI crypto proposal the data can be verified when the tag is gone. However the symmetric key management and secrecy remain a challenge in open loop systems.
- Digitally signed data as provided for by ISO/IEC 20248 ➔ **strong** if we can trust the **TID**. Data is verifiable even when the tag is gone.

To **kill** or not to kill a tag. Killing a tag removes all access to the tag. A killed tag can not flood and be acid RAIN.

The RAIN Reader Communications Interface (RCI)

is designed on the premise that the application knows

which tags it wants to read, the type of tag and how to access it. This is called tag spotting.

The application instructs the reader of the targeted tags using SpotProfiles.

SpotProfiles contain a mask for the targeted tag, access instructions and reporting instructions.

An RCI reader will therefore ignore all unwanted tags.

This is possible only if we all use standard data structures.

Non-standard data structures will interfere and be interfered with.

It is in all our interest to be good RAIN neighbours.

GS1 examples

A standard 96 bit GS1 tag

MB-01 PC Word					MB-01 UII/EPC
EPC len	UserMem	XI	Standard	RFU	EPC as specified by GS1
00110	0	0	0 (GS1)	0x00	96 bits

A standard 96 bit GS1 tag with attribute data

MB-01 PC Word					MB-01 UII/EPC	MB-11 User Memory	
EPC len	UserMem	XI	Standard	RFU	EPC as specified by GS1	DSFID	Data fields according to ISO/IEC 15961 & 15962
00110	1	0	0 (GS1)	0x00	*96 bits*	8 bits	*≥ 0 bits*

A standard 96 bit GS1 tag with ISO/IEC 20248 attribute data

MB-01 PC Word					MB-01 UII/EPC	MB-11 User Memory			
EPC Len	UserMem	XI	Standard	RFU	EPC as specified by GS1	DSFID	DAID	CID	signature, timestamp and company defined attributes
00110	1	0	0 (GS1)	0xXX	*96 bits*	0x11	*32-48 bits*	*16 bits*	*≥ 0 bits*

Note the TID is not shown.

ISO examples

A standard 96 bit ISO tag.

MB-01 PC Word					MB-01 UII/EPC
UII len	UserMem	XI	Standard	AFI	UII as specified by ISO
00110	0	0	1 (ISO)	0xXX	96 bits

A standard 96 bit ISO tag with attribute data.

MB-01 PC Word					MB-01 UII/EPC	MB-11 User Memory	
UII len	UserMem	XI	Standard	AFI	UII as specified by ISO	DSFID	Data fields according to ISO/IEC 15961 & 15962
00110	1	0	1 (ISO)	0xXX	*96 bits*	8 bits	*≥ 0 bits*

A standard 96 bit ISO tag with ISO/IEC 20248 attribute data.

MB-01 PC Word					MB-01 UII/EPC	MB-11 User Memory			
UII Len	UserMem	XI	Standard	RFU	UII as specified by ISO	DSFID	DAID	CID	Signature, timestamp and company defined fields
00110	1	0	1 (ISO)	0xXX	*96 bits*	0x11	*32-48 bits*	*16 bits*	*≥ 0 bits*

Note the TID is not shown.

ISO/IEC 20248 examples

The smallest standard compliant digital twin tag. This data structure is fully interoperable with all ISO and GS1 tags. It provides for untracability.

MB-01 PC Word					MB-01 UII/EPC	MB10 TID
UII Len	UserMem	XI	Standard	AFI	DAID	
00010	0	0	1 (ISO)	0x92	32 bits	32-96 bits

An ISO/IEC 20248 using null encryption. The tag owner/issuer and data structure are verifiable and decode into named fields.

MB-01 PC Word					MB-01 UII/EPC		
UII Len	UserMem	XI	Standard	AFI	DAID	CID	Company defined fields
XXXXX	0	0	1 (ISO)	0x92	32-48 bits	16 bits	*≥ 0 bits*

A verifiable attribute tag.

MB-01 PC Word					MB-01 UII/EPC			MB-11 User Memory
UII Len	UserMem	XI	Standard	AFI	DAID	CID	Company defined fields	Signature, timestamp and company defined fields
XXXXX	1	0	1 (ISO)	0x92	32-48 bits	16 bits	*≥ 0 bits*	≥ 256 bits

Note the TID is not shown.

That’s all. Questions?