RAIN RFID Solutions: Integrity, Privacy and Trust

Whitepaper

V.1.0

October 2019

RAIN Alliance Whitepaper: RAIN RFID Solutions: Integrity, Privacy and Trust

1. Introduction

RAIN RFID is a wireless technology that connects billions of everyday items to the internet, enabling businesses and consumers the ability to identify, locate, authenticate and engage each item.

Privacy and data security are both important facets of any technology solution design. This document highlights some of the potential issues when using RAIN systems and provides a high-level guide to a wide range of tools and features used to protect RAIN deployments.

2. Why should I care about security in a RAIN system?

The RAIN technology benefits of identifying, locating, authenticating, and engaging with everyday items depend on the exchange of small amounts of data. While RAIN tags hold significantly less data than many other computing or storage devices, they often act as the sole link between a physical item and a sophisticated backend data processing system. Therefore, RAIN tags, and the data they carry, are vital to the integrity of a deployment. The accompanying risks associated to a solution, can be summarised in three main groups:

Data integrity issues: caused by inaccurate data on the tag that can impact correctness, stability and performance of a system.

Data privacy issues: caused by data being accidently or maliciously used in unintended ways.

Trust issues: caused by system participants being unsure that the tags and items are genuine.

Let's take each of these risks in turn.

2.1. Data integrity issues

Systems are only as accurate as the data and processes they use, and data integrity is vital for systems such as those monitoring physical asset movement or managing inventories. If the data injected into the system is erroneous due to a tag not having the intended identifier, the system will be inaccurate and the connection between the physical world and digital world will be broken. In the case of single tag errors in inventory systems, this can lead to items never being 'found' and therefore never replenished or, on the opposite end of the scale, additional items being reordered so there is more inventory than necessary.

If tag data has been modified or erased, or arguably worse, not properly encoded in the first place, the tagged items will not be counted and therefore systems will be inaccurate. Whilst this does not sound too serious for single items; this may leave opportunities open to compromise tags if security has not been considered in the complete solution design. This could ultimately result in loss of inventory accuracy, loss of revenue, operational inefficiencies and customer dissatisfaction.

2.2. Data privacy issues

Recent changes in legislation and some high-profile cases have raised the issue of data privacy in the public consciousness. Ensuring individuals have control of their own data is considered a moral obligation for most system owners and, in many areas of the world, a legal necessity (with the European Union leading the way by introducing the GDPR[1] regulations). The use of RAIN technology can be one step in addressing data privacy issues.

Whilst RAIN tags do not contain vast amounts of data, they are typically linked to a specific physical item; in turn this item would often be used by an individual. Be it a consumer product, pharmaceutical item, computing device, or any number of other physical things, when combining data collected with other systems it is plausible to record information pertaining to individuals. By themselves, RAIN tags do not hold personal identifying data; however, the combination of item tag data and data from other sensors or systems, may allow unscrupulous individuals to piece together the movements and preferences of individuals. Whilst this activity is unlikely and would require considerable effort, a range of mechanisms to combat this are supported by RAIN technology.

2.3. Trust issues

Consumers want to know the products they have purchased are genuine. For example, a customer might want reassurance the designer bag purchased is authentic or the sports jersey is an officially licensed product. Arguably more important is trusting the medications being provided are authentic and at every stage in the supply chain they can be proved to be from a reliable source. This way not only will the patient have trust in the specific item, the medical practitioners will also have trust in the whole system.

There are other significant use cases where the authenticity of items is important for both the system and individuals; take the case of vehicle identification on stretches of toll roads or as part of a vehicle tax system. There is great convenience in having an automated system for both the driver and the system owner or government; but, both sides of this transaction must trust fraud is not possible within the system. For the operator, security measures are essential to ensure tags are not hacked or cloned; but this is also vital to the users as they do not want their own tags being cloned resulting in additional fees being added to their account.

Proving authenticity is important for product manufacturers; companies must ensure they are using genuine parts during the manufacturing process. This is critical for product quality and consumer confidence. But, equally as important is parts authenticity for aftermarket use, ensuring consumers can purchase safe in the knowledge that spare parts and upgrades are officially provided by the original manufacturer.

These are just a few examples where proving authenticity is important to all participants within a system and shows trust is a vital component to successful system design and sustained usage.

3. What can be done about these risks and opportunities?

The good news is there are many mechanisms within the prevailing standards upon which RAIN technology is built to manage the risks and potential problems highlighted earlier. In fact, many of the

[1] General Data Protection Regulation (GDPR): https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

risks are already well known from other wireless technologies and so RAIN can address the risks through well-known solutions as well as through some solutions exclusive to RAIN technology.

3.1. Basic data protection

The most basic form of system protection is to ensure it is not possible to change the data on the tag. Fundamentally, the most relevant piece of information on a RAIN tag is the unique number encoded within its memory; this is usually one of either an ISO Unique Item Identifier (UII) or a GS1 Electronic Product Code (EPC). By default, this memory bank is modifiable since the brand or process owner will typically own this data. However, this means anyone can write or modify the data within the UII/EPC memory bank unless some form of protection has been undertaken.

To protect both end users and the integrity of RAIN systems, it is possible to lock the data on a RAIN tag. This locking mechanism will ensure the tag cannot be altered without a password, or it can also be locked such that its data can never be changed.

Whilst all the memory banks can be locked, of critical importance are the Reserved and UII/EPC memory banks. The UII/EPC memory usually holds the most important data for the tag, and therefore data integrity of the system is at stake if this is altered. The Reserved memory bank contains the passwords that allow the tag to be locked and unlocked, it also contains the password required to enact the Kill functionality. The tag is unlocked in the default state and the effects of locking each memory bank can be seen in the table below:

		Unlocked (& default)		Locked[2]	
		Readable	Writable	Readable	Writable
Memory Bank[3]	TID	☑	☒	☑	☒
	UII/EPC	☑	☑	☑	☒
	Reserved	☑	☑	☒	☒
	User memory	☑	☑	☑	☒

The mechanism and commands to complete these actions are beyond the scope of this document, but all are described and standardised in the global Gen2v2 specifications.

But, why should system owners bother with this locking process? Well, this is the most elementary layer of protection provided by most RAIN tags. Leaving tags unlocked is akin to not setting up a computer password and potentially opens the system to accidental or deliberate abuse.

[2] Tags can be locked such that it is possible to be unlocked by use of a password; or tags can be permanently locked resulting in the data never being able to be modified.

[3] TID - Tag IDentification number, UII - Unique Item Identifier, EPC - Electronic Product Code

3.2. Protecting users, bands and system integrity

Beyond the basic locking protection of the system there are several mechanisms intended to protect all participants within a system. Firstly, let's look at those designed primarily for the protection of user privacy. Secondly, we will look at options for protection of authentication.

3.2.1. User privacy

As described previously, systems must consider the privacy of users and public in all design and implementation. Of course, RAIN tags do not hold significant amounts of data, but they can, and often do, hold a unique data structure that could point to information that could be considered personal. Amongst other things, the GDPR regulations in Europe consider an individual's location and online identifier as personal data[4].

The methods of protecting consumer and user privacy range from basic physical actions to more sophisticated tag IC based methods. Some of these include:

Physical removal: Simply removing the tag from the originally tagged item is one of the suggestions of early privacy impact assessments[5] (PIA). Certainly, this is relatively easy to do when tags are not embedded into items. However, some benefits of using a RAIN tag may be lost including, for example, opportunities for pre- and post-sale use, for returns, consumer interaction and EAS applications.

The physical removal method has the disadvantage of requiring additional process; therefore, impacting operations. This method is also clearly not possible in some of the increasingly common implementations where tags are embedded into items, therefore, removing the tag is simply not possible.

Kill Command: All RAIN tags support the Kill command. This provides a mechanism to render the tag permanently unusable. By issuing a Kill command, a reader instructs the tag to enter the 'killed' state, where it will not respond to a reader in any way or under any circumstances. There is no way to reverse this operation, therefore, like the physical removal of tags, the RAIN tag cannot be used for retail returns or any other application using the RAIN tag.

Untraceable Command: The optional Untraceable command has been designed to be reversible, but, only by authorised users with the credentials to do so. The supported functionality of Untraceable

[4] https://ec.europa.eu/justice/smedataprotect/index_en.htm

[5] https://www.gs1.org/standards/epc-rfid/pia

can vary from tag to tag, but the two main potential effects are range reduction and the ability to hide parts of the memory banks.

Range reduction does exactly what the title suggests, it reduces the operating range at which the tag can be read. The range is reduced to the level where the tag can only be read when it is very close to the reader antenna, reducing the possibility of being able to read tags from a distance.

As well as enabling and disabling range reduction with persistence, it is also possible to toggle the functionality temporarily. When toggling the range reduction, the range reduction mode will be reversed until the tag loses power, reverting to its previous persistent state when it next powers up. This functionality opens many use cases to engender consumer confidence whilst still allowing the tags to be utilised post sale.

The *show/hide* part of the Untraceable command allows systems to hide parts of a tag memory bank. It is possible to hide all or some parts of the EPC bank, all or part of the TID and all the user memory.

When the UII/EPC memory bank is untraceably hidden only part of the memory bank is visible with the tag only retuning the unhidden data. For example, it may be set to hide the serialised number. This way, no individually identifiable data can be obtained. In the same way, the TID can be hidden in part or totally. If hiding part of the TID code, the serial number of the tag will be hidden leaving the class ID and other chip specific data exposed. This allows systems to operate normally with the possibility to identify the type of tag silicon without any serialised data being visible. Again, this is intended to ensure no unique data can be associated to an individual whilst still allowing systems identify and use differing functionality from diverse range of tag chips. Finally, if a tag contains user memory, this too can be hidden using Untraceable. In this case, it is all or nothing in terms of hiding or exposing the data.

If parts of the memory are set to untraceable, these memory banks will act as though they do not exist. When systems attempt to access a memory bank that has been hidden, the tag will return an error condition stating a memory overrun.

A tag can only execute the Untraceable command when it is in, what is known as, the secured state; therefore, if a non-zero access password has been encoded into the tag, it is required to use the Untraceable feature.

Whilst it is possible to hide all the data from these memory banks, keeping some data exposed is recommended. As a minimum it is recommended to hide only part of the UII/EPC number and the TID memory banks. This will ensure the presence of tags can be identified and interacted within a system whilst still hiding the unique identifiable part for the data.

3.2.2. Ensure you are talking to the right tag by authenticating identities

Solutions should be designed to consider the authentication of tags and the connections to the system where appropriate. There are many applications where knowing to whom we are engaging with is critical to ensure a level of comfort with the type of information exchange. For example, when communicating with banks about finances, they want to make sure they are really talking to the account holder, and you want to ensure you are really talking to them! Are 'they' really the authorised banking entity or is it some other intermediary trying to gain access to your finances?

For RAIN RFID systems similar issues arise. There are many applications where we care about the authenticity of products, items and consumables etc. If you purchase an item of clothing, you might care about its authenticity. As a government, you are likely to care that citizens driving along the

highways display number plates that are authentic and that tax has been paid. As a manufacturer of high-tech parts, it may be important customers can have confidence parts are fit for purpose, for example in aircraft or vehicles. As an access provider, it is vital that only authorised people or vehicles enter the premises.

How can we ensure this authenticity?

There are several ways RAIN systems can be used to address the issues above; from the from very simple to the more sophisticated.

The UII/EPC number is often considered as the "license plate", a unique identifier and pointer to the item's data within the system. However, without further protection, this can be easily replicated by simply encoding a duplicate tag. An improved method might be to link the TID to the UII/EPC within the system. Since the TID cannot be modified by a user, a simple database or a dedicated TID serial number range might be used to verify that a tag presents the correct TID and UII/EPC combination. Whilst it is a relatively simple idea, this requires some data synchronisation and adds complexity to implementations. More importantly, while this might help ensure that tag data cannot be easily modified or duplicated, it remains feasible to replicate both the TID and the EPC within the system. Every time the tag is read the same static data is transferred to the reader.

As an additional safeguard, some tags provide a "digital signature" on the tag data. This can help ensure that tag content has not been changed, thereby allowing system owners to be comfortable with the authenticity of the data received. However, important to note is that the data passed over the air interface remains static which, could leave the system potentially vulnerable to cloning or tracking.

Some RAIN RFID tags can authenticate identities using cryptographic algorithms where information changes over the air interface dynamically.

Some RAIN RFID tags can authenticate identities using cryptographic algorithms where information changes over the air interface dynamically. Using established cryptographic techniques, the reader and the system can be assured of the authenticity of different components using keys that are only known to the system.

Cryptographic RAIN tags can secure transactions by using secret keys that guarantee tag authenticity and can also encrypt transaction data. Keys are stored within a special secure vault in the tag silicon which is not accessible; ensuring a high level of system security.

The process of authenticating a tag using a RAIN reader is relatively straightforward. A challenge is sent to the tag which is then processed by the tag's secure cryptographic engine. The response that is returned to the reader can be verified against a secret key ensuring authenticity. Whilst the information on the tag remains the same, the data transmitted over the air changes during each transaction. Such data cannot be predicted or usefully cloned by an attacker without the key. Also, the standards allow for cryptographic encapsulation of other commands such as Untraceable and Kill providing extra security when interacting with tags.

There are many options to securing of the information held in RAIN tags. Cryptographic tags offer a high degree of protection against cloning and other attacks, though the added protection provided can require a more complex system design. RAIN can be used to authenticate tags in even in the most demanding environments, for instance reading tags on fast-moving vehicles in highway applications.

Indeed, solution designers today are very accustomed to considering questions of security, authenticity and privacy. These needs can be satisfied while retaining the system efficiencies, performance and economics advantages of deploying RAIN RFID.

4. Summary and best practices

Security, authentication and privacy in solution design is clearly very important and RAIN technology products and systems have been developed such that these considerations are given high priority. Whilst the amount of data on an individual tag may be small, this data can be critically important to the integrity of a system.

To ensure the privacy of users and integrity of the system, some simple best practices should be employed:

- Always assign unique passwords for kill and access functionality by overwriting the default settings; then make sure it is locked!
- Don't use the same password for every tag, they should be dynamic (based on TID or some other formula ensuring the password is different for every tag).
- Whenever in doubt, use cryptographic authentication to secure your tags' identities.

Leaving tags unlocked is not an option due to the potential for data integrity abuse and therefore, as a minimum, locking the tags should be considered a necessity in every system design. Other optional methods to address data security and privacy such as Untraceable and Kill are available and designed to protect privacy of end-users with varying levels of permanence and complexity depending on the use case.

Cryptographic tags offer the highest level of security possible with the ability to ensure authenticity of the tag and its data.

Many options and functions address the security, authenticity and privacy challenges in RAIN solutions. Solution designers can use any of these tools in combination and should choose those most appropriate to balance the system complexity and performance against the security and privacy risks.

5. Background and contributors

This document was developed within the RAIN RFID Technical Workgroup with the following contributors:

Main author:

James Goodland	(NXP Semiconductors)

With contributions from:

Josef Preishuber-Pflügl	(CISC Semiconductor)
Matthew Robshaw	(Impinj)
Jim Springer	(EM Microelectronic)

6. ABOUT RAIN ALLIANCE

The RAIN 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 Alliance

One Landmark North
20399 Route 19
Cranberry Township, PA 16066

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