RAIN Solutions
Data Integrity, Privacy, and Trust

2nd version

March 2026

DISCLAIMER: This document, and all other information, materials, or services, if any, provided by RAIN Alliance in connection with this document, are provided "as is," and RAIN Alliance makes no representations or warranties, express, implied, statutory, or otherwise, and expressly disclaims any representation or warranty that implementation of any technical or business specifications or methods portrayed in this document will not infringe any third-party intellectual property rights, as well as any implied warranties of merchantability, fitness for a particular purpose, correctness, accuracy, reliability, or any equivalents under the laws of any jurisdiction that might arise from products, activities, or information disclosures relating to this document, or any act, omission, or requirement by any third party. If you do not understand or agree with the foregoing, you should not access this document or implement any element of it.

Why Should I Care About Security and Privacy in a RAIN System?

The benefits of RAIN technology - identifying, locating, authenticating, and engaging with everyday items - rely on the exchange of small amounts of data. Though 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 along with the data they carry are vital to the integrity of a RAIN system deployment. The accompanying risks associated with a solution can be summarized into three main categories:

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

Privacy issues: caused by data being accidentally or maliciously used in unintended ways.

Trust issues: caused by uncertainty among system participants about whether the tags and items are genuine.

Let's examine each of these risks in turn.

1.1 Data Integrity Issues

Systems are only as accurate as the data and processes they use, and data integrity is vital for systems that monitor physical asset movement or manage inventories. If the data injected into the system is erroneous – for example, if a tag does not have the intended identifier - the system will become inaccurate, and the connection between the physical and digital worlds will be broken. In inventory systems, even a single tag error can result in items never being "found" — and therefore never replenished — or, conversely, in additional items being reordered, leading to excess inventory.

If tag data has been modified, erased, or arguably worse, not properly encoded in the first place, the tagged items will not be counted, resulting in system inaccuracies. While this may not seem serious for individual items, it can create vulnerabilities if security has not been considered in the overall solution design. Ultimately, this could lead to inventory inaccuracy, revenue loss, operational inefficiency, and customer dissatisfaction.

1.2 Data Privacy Issues

Recent changes in legislation and some high-profile cases have raised the issue of data privacy in the public consciousness. Ensuring that individuals have control over their personal 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).

Smartphones have re-shaped how we live — enabling us to navigate, communicate, shop, and work with ease. By and large, the general public accepts that smartphones collect detailed behavioral data: where we go, what we browse, who we interact with – effectively making them one of the most powerful surveillance tools ever created! Despite these trade-offs, their usefulness is rarely questioned because the benefits outweigh the risks.

RAIN is a technology used to identify physical objects and connect them to the digital world. It is limited in scope and function. It has no microphone, no camera, and no GPS.

Nonetheless, some concerns about RAIN and privacy persist — often based on misunderstanding or incorrect assumptions.

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. Whether it's a consumer product, pharmaceutical item, computing device, or any other physical object, combining data collected from various systems can plausibly result in the recording of 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.

1.3 Trust Issues

Consumers want reassurance that the products they purchase are genuine. For instance, a customer may seek confirmation that a designer bag is authentic or that a sports jersey is officially licensed. This desire for authenticity becomes even more critical when it comes to medications. Patients need to trust that the drugs they receive are genuine, and that every stage of the supply chain can verify their origin and reliability. Ensuring this not only builds confidence in the specific product but also strengthens trust in the entire healthcare system—for both patients and medical professionals.

There are other significant use cases where authenticity is crucial for both individuals and systems. Consider vehicle identification on toll roads or within a vehicle tax system. Automated systems offer great convenience to both drivers and system operators, including government entities. However, this convenience must be matched by trust—both parties need assurance that fraud is not possible within the system. For operators, robust security measures are essential to prevent tags from being hacked or cloned. Equally important, users must be confident that their own tags cannot be duplicated, which could result in unauthorized charges to their accounts.

Proving authenticity is essential for product manufacturers. Companies must ensure that genuine parts are used throughout the manufacturing process, as this is critical for maintaining product quality and consumer confidence. Equally important is the authenticity of parts in the aftermarket. Consumers need to be assured that the spare parts and upgrades they purchase are officially supplied by the original manufacturer, allowing them to buy with confidence and trust in the safety and reliability of those components.

These are just a few examples that highlight how proving authenticity is essential for all participants within a system. They demonstrate that trust is a foundational element of successful system design and sustained usage.

2. How to Mitigate Risks

RAIN tags primarily store a unique identifier for an item. This identifier acts as a digital fingerprint and is used to link to a database containing more detailed information about the item such as its type, manufacturer, or other relevant data. By enabling this connection, RAIN tags facilitate efficient tracking and management of items throughout the item life cycle.

RAIN tags do not store personal information about individuals**.** They hold data exclusively related to the tagged item. This distinction is crucial. RAIN technology supports item-level tracking and management without compromising individual privacy.

The good news is that the prevailing RAIN technology standards include many mechanisms to manage the risks and potential problems highlighted earlier. In fact, many of these risks are already well known from other wireless technologies. This means RAIN can address these risks by leveraging proven, well-established solutions and by offering innovative safeguards unique to RAIN technology.

2.1 Basic Data Protection

The most basic form of system protection is ensuring that data on the tag cannot be tampered with or wrongfully altered. The most relevant piece of information on a RAIN tag is the unique number encoded within its memory. This is 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 usually controls this data. However, this does not mean that anyone can write or modify the data within the UII/EPC memory bank as system integrators and service bureaus use the protection mechanisms in place to safeguard the information on the tag.

Indeed, to protect both end users and the integrity of RAIN systems, it is mandatory for the service bureau operator to lock the data on a RAIN tag after encoding. This locking mechanism ensures that the tag cannot be altered without a password. In many cases, the tag will be permanently locked, meaning its data can never be modified.

Whilst all the memory banks can be locked, two are of critical importance: the Reserved and UII/EPC memory banks. The UII/EPC memory usually holds the tag's most important data, and therefore data integrity of the system is at stake if this is altered. The Reserved memory bank contains the password required to lock and unlock the tag, as well as the password required to activate the Kill functionality, which permanently disables the tag. Initially at factory settings, a RAIN tag is in an unlocked state, meaning its data can be modified unless protective measures are applied.

The effects of locking each memory bank are summarized in the table below:

[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

		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 defined in ISO/IEC FDIS 18000-63 parameters. The vendor that programs the manufacturer identifier (MDID number) needs to be the one to lock the TID.

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

2.2 Protecting Users, Brands, and System Integrity

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

2.2.1 User Privacy

As described previously, systems must consider the privacy of the users in all aspects of design and implementation. While RAIN tags do not hold significant amounts of data, they often contain a unique identifier that can point to information that may be considered personal.

Under the General Data Protection Regulation (GDPR) in Europe, an individual's location and online identifier are considered personal data.

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

Kill Command – an irreversible mechanism that renders the tag permanently unusable.

Untraceable Command – a reversible command that obscures or hides tag's data and/or reduces the operating range.

More information on these commands is available in **Appendix 1.**

2.2.2 Ensure You Are Talking to the Right Tag by Authenticating Identities

The authenticity of products, items, and consumables may be critical for some applications. For instance, public authorities need to ensure that vehicles on public highways display authentic license plates and that taxes have been paid. Manufacturers of high-tech components, especially in sectors like aerospace or automotive must ensure that customers can trust parts are fit for purpose and not counterfeit. Likewise, access control systems must guarantee that only authorized individuals or vehicles are permitted entry.

There are several ways RAIN systems can address authenticity concerns, ranging from very simple methods to more sophisticated mechanisms. These are covered in detail in **Appendix 2**.

3. Summary and Best Practices

Security, authentication, and privacy are critical considerations in solution design, and RAIN technology products and systems have been developed with these priorities in mind. While the amount of data stored on an individual tag may be small, it can be crucially important to the overall integrity of the system.

To safeguard both user privacy and system integrity, it is essential to follow some simple best practices, including:

- Always assign unique passwords for both kill and access functionalities by overwriting the default settings. Once configured, ensure the tag data encoded is properly locked.
- In critical applications, use cryptographic authentication to secure your tags' identities.

Leaving tags unlocked is not an option because of the risk of data integrity abuse. At a minimum, locking tags should be considered a fundamental requirement in every system design. Additional methods such as Untraceable and Kill functionalities are available to enhance data security and privacy. These features are specifically designed to protect end-user privacy, offering varying levels of permanence and complexity depending on the use case.

Cryptographic tags provide the highest level of security, ensuring both the authenticity of the tag and the integrity of its data.

Many options and functions address the security, authenticity, and privacy challenges in RAIN solutions. Solution designers can combine these tools as needed, selecting those most appropriate to balance system complexity and performance against the associated security and privacy risks. To evaluate these risks and to take appropriate actions, solution designers are encouraged to conduct a Privacy Impact Assessment (PIA). The complete process is described in standard EN 16571: Information technology - RFID privacy impact assessment process.

4. Background and Contributors

Version 1 of this document was originally developed in 2019 within the RAIN Alliance Technical Workgroup with the following contributors:

Main author:	James Goodland	(NXP Semiconductors)
With contributions from:	Josef Preishuber-Pflügl	(RAIN Alliance)
	Matthew Robshaw	(Impinj)
	Jim Springer	(EM Microelectronic)

Version 2 was produced in September 2025, augmenting the original documentation with additional information related to technological trends towards an increasing number of embedded RAIN tags in recognition of emerging legislation such as DPP, and in anticipation of RAIN-enabled smartphones becoming available on the market in the not-too-distant future.

Contributions from:	Bertus Pretorius	(Toennjes)
	Swapnil Agarwal	(EM Microelectronics)
	Claude Tetelin	(GS1 Global)

Appendix 1 – More information on Kill and Untraceable Commands

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 authorized users with the credentials to do so. The supported functionality of Untraceable 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.

Hide parts of the memory bank: 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 serialized 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.

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

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

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.

Hiding all tag memory is technically possible but operationally undesirable. A more balanced approach is to hide only the uniquely identifying portion of the UII/EPC and, where applicable, the serialization portion of the TID. This preserves core system functionality—such as tag presence detection, filtering, and process control—while protecting uniquely identifiable tag elements that could be associated with an individual

Appendix 2 – Ensuring Authenticity

There are several ways RAIN systems can be used to ensure authenticity; from the 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 synchronization 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 (see ISO/IEC 20248 – *DigSig)*. 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 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 (see ISO/IEC 29167). 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 Untrac (eable 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 technology.

About the RAIN Alliance

The RAIN Alliance enables organizations to improve traceability, effectiveness, and sustainability by simplifying, standardizing and accelerating the adoption of RAIN technology through global collaboration and innovation. Its global membership consists of companies and organizations which develop and deploy RAIN technology solutions across many vertical markets.

RAIN is a standards-based wireless technology that enables businesses and consumers to identify, locate and authenticate billions of items connected to the Internet of Things. RAIN technology uses the ISO/IEC 18000-63 protocol (also known as GS1 UHF Gen2).

For more information, please visit therainalliance.org