

# How to prevent sabotage and ensure consumer privacy with RAIN RFID

---

Danny Haak





# By default, RAIN RFID tags are not protected

---

Everybody is able to re-write the EPC and other memory contents

Everybody is able to kill the tags





# There are two ways to protect RAIN RFID tags

---



Passwords



Lock

# Two passwords

---



## **Access password**

used for (preventing) reading and writing specific memories in the chip

## **Kill password**

used for (preventing) killing the chip



# Lock provides four options

---



1. Write (and read) the memory - without Access Password
2. Write (and read) the memory - when providing Access Password
3. Impossible to write (and read) the memory - even while having the Access Password
4. Always write (and read) the memory

Independent setting for both passwords, EPC, User and TID memory



A woman with long brown hair is looking thoughtfully to the side in a clothing store. Above her head is a large, light blue thought bubble graphic. The store background shows shelves of folded clothes and a mannequin.

# Privacy is getting more and more important

---

Consumer attention is growing

Retailers move from tickets to embedded tags



# RAIN RFID poses privacy risk

---

Longe range identification

Globally unique number (TID)

Associated with or integrated in physical product

**‘Indirectly identifiable personal information’**

Verwerk ik als organisatie persoonsgegevens met wifitracking en bluetoothtracking?

Ja. Met wifi- en bluetoothtracking verzamelt u een combinatie van gegevens waarmee iemand te identificeren is. En dat betekent dat deze gegevens persoonsgegevens zijn.

Bij wifi- en bluetoothtracking verzamelt u doorgaans iemands MAC-adres (het unieke nummer van een telefoon of ander mobiel apparaat), de signaalsterkte van het geregistreerde wifi- of bluetoothsignaal, het serienummer en/of de locatie van de sensor en het tijdstip van de waarneming.

Van direct identificerende gegevens is in dit geval geen sprake. Het gaat hier niet om gegevens als namen, adressen en telefoonnummers. Een enkel MAC-adres op zichzelf onthult ook niet direct de identiteit van een persoon.

Toch zijn het persoonsgegevens. We noemen dit indirect identificeerbare persoonsgegevens. Dat komt omdat u de gegevens kunt combineren met elkaar of met andere gegevens. Zo kunt u de gegevens terugbrengen tot een bepaald persoon.

Aanvullende gegevens waarmee u mensen indirect kunt identificeren zijn bijvoorbeeld camerabeelden, betalingsgegevens in winkels, inloggegevens van openbare wifi-hotspots of het gebruik van toegangspoortjes met unieke identificatoren, zoals RFID-tags.





# RAIN RFID privacy features

---

‘Untraceable’

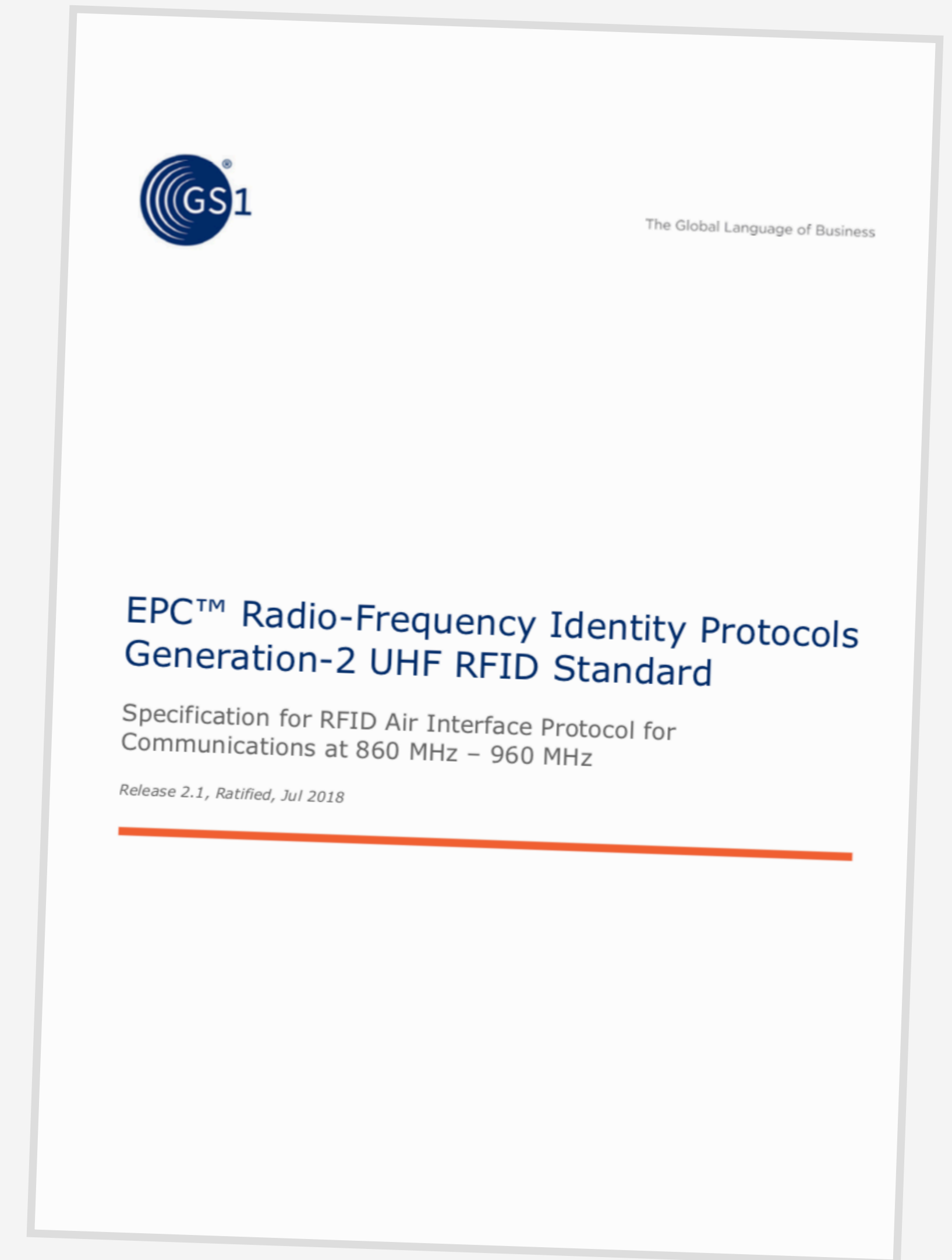
- **Read Range Reduction**

Read only at short distance

- **Hide Memory**

Only read privacy-sensitive data when knowing the Access Password

Works even with permanently locked memories; protected with Access Password





“It is enough to permanently lock the EPC memory and passwords to secure a tag.”

– Lots of people





Nope. You need a password.

---

\* Some RAIN RFID ICs allow you to enable Untraceable on a permalocked tag with a zero-valued password.



# Using the same password for all tags is wrong

---

Once the password is leaked, a villain can kill all your tags.

- **Lots of people will know it**  
Service bureaus, retail partners, etc.
- **Eavesdropping**  
Password is sent unencrypted between reader and tag
- **Brute-force**  
Takes a few years... but hey...

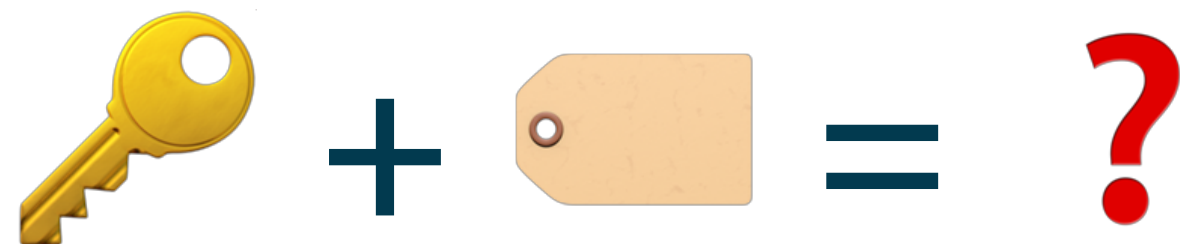
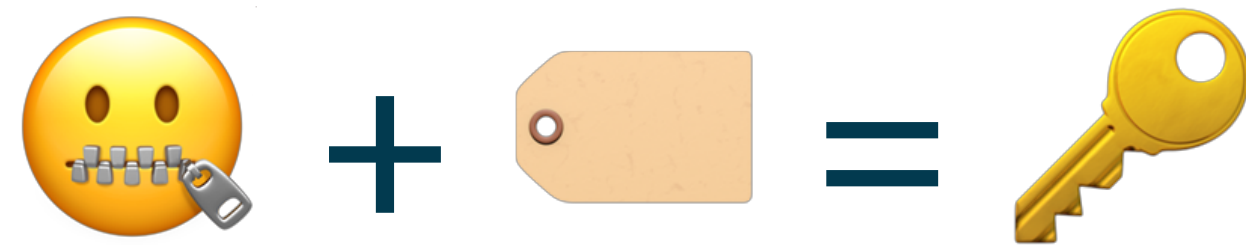




# Cryptographic Hash is the solution

---

Secret 🗝️, EPC 🏷️, Password 🔑



When somebody knows the password for one tag, it is useless for other tags.



# Example

---


See for yourself at:

<https://mimasu.nl/tag-encoding/tag-security>


EPC in hexadecimal format

 3074257bf7194e4000001a85

Secret in hexadecimal format

 8fc590ee628448b4893a70fd5a6252bb

Password in hexadecimal format

 4bc9c49c

Set example

Clear



# The secret is safe. Promised.

---

**It is not stored directly in the tag, nor communicated over the Air Interface.**

Follow (security) industry best practises for managing the secret.

**It is not necessary to distribute the secret to 3rd parties.**

Build an API where you input the EPC , get the password  in return.



# Cryptographic Hash and Untraceable

---

**Read Range Reduction** is compatible with the Cryptographic Hash scheme. You can still retrieve the EPC to calculate the password.



**Hide Memory** is *not* compatible with the Cryptographic Hash scheme. You cannot obtain the EPC, so you cannot calculate the password.



\* Some RAIN RFID ICs only allows enabling Read Range Reduction at a very short range.



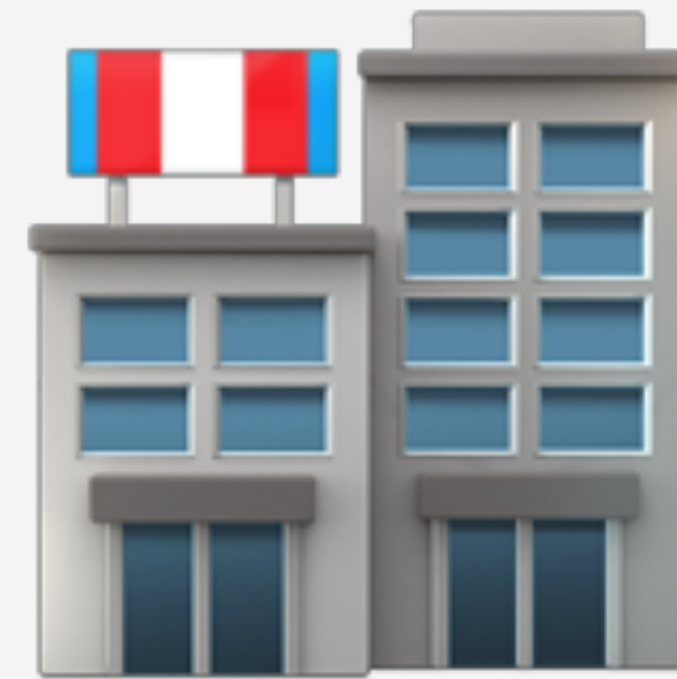
# Retail example

---



Brand

Brand encodes tag with passwords based on the secret and lock



Retail store

Retail store enables Untraceable - calculates Access password based on the secret and the EPC



Consumer

Consumer is able to temporarily undo Untraceable by using API of the brand





Want to know more?

Danny Haak | [danny.haak@nedap.com](mailto:danny.haak@nedap.com)