How to prevent sabotage and ensure consumer privacy with RAIN RFID

Danny Haak

nedap
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
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’
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 🪪

 porém + 🛢️ = 🪪

🔑 + 🛢️ = ❓

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
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