# Security and Reliability of Automated Waste Registration in The Netherlands

Dick Visser Thijs Kinkhorst

February 2008

Universiteit van Amsterdam

Research report for System and Network Engineering, University of Amsterdam, the Netherlands. Conducted under supervision of Jeroen van Beek, Marc Smeets and Hans IJkel from KPMG IT Advisory, ICT Security & Control.

**Abstract**

Electronic registration of domestic waste is in wide use, often to raise taxes based on the amount of waste households produce, but not much prior research into the technical aspects of this area has been done. Two basic methods are found: personal household containers and shared underground containers. This report tries to define requirements for such systems and compares several systems in actual use to these requirements.

Every municipality surveyed employed a different combination of systems, each having their own strengths and weaknesses. All use radio frequency identification (RFID) but many can easily be copied. Encryption is hardly used. No critical security risks were found, but a number of issues still need addressing.

# Contents

# 1 Introduction

## 1.1 Waste collection

Handling waste is an important part of modern life. In 2006 more than ten million tons of waste were collected by Dutch municipalities. Disrupting this collection process could have serious effects on society.

A disturbing example of such disruption can be found in the Italian city of Naples, where in 2007–2008 corruption and political incompetence have caused waste collection to stop, leading to chaos and even riots in the streets[1]. In 2005 Amsterdam waste collection personnel went on strike which almost led to the cancellation of the 5-yearly event Sail[2].

Meanwhile the volume of collected waste keeps increasing, as depicted in figure 1 [3].

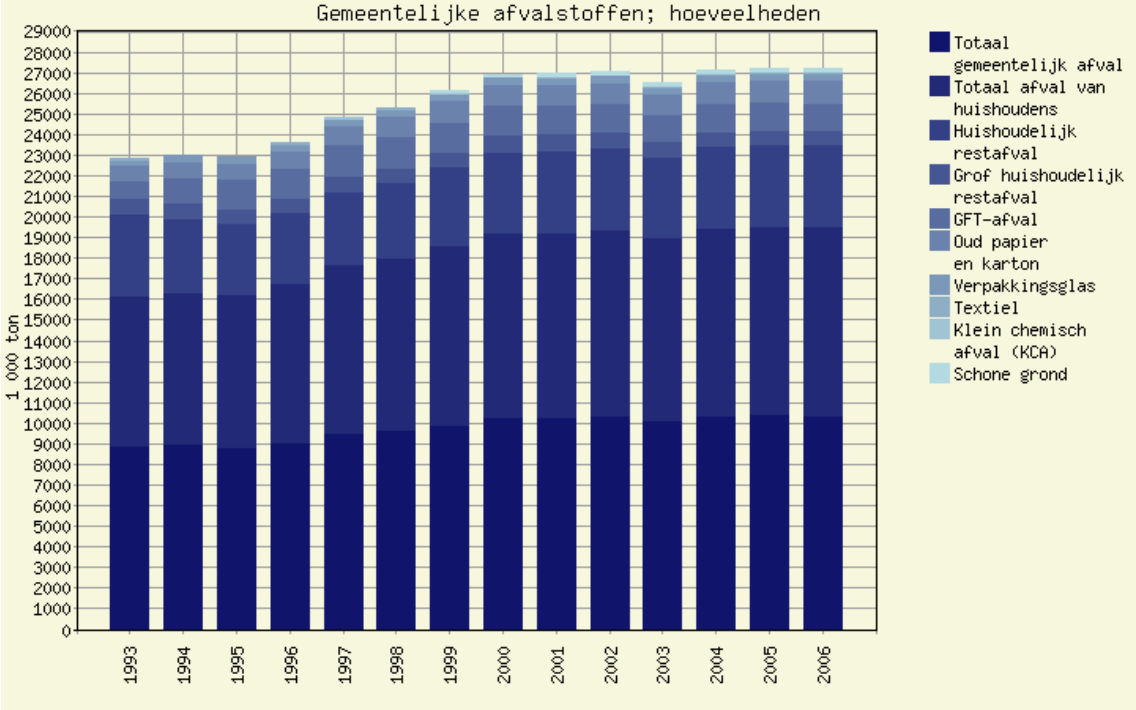


Figure 1: Municipal waste; quantities (source: CBS)

The increasing amount of waste, stagnation of the waste separation level[4], and an increased focus on environmental aspects have made many municipalities realise that they need a better and more efficient system of waste collection.

Many municipalities encourage waste separation by introducing differentiated tariffs or *diftar*, meaning there is some kind of relationship between the amount of waste one disposes of and the price paid. A household pays per amount of waste, while fractions like glass and paper are free of charge. In 2002 about one in four municipalities employed diftar, and the number is expected to grow[5]. One way of applying diftar is to make the use of specially taxed waste bags mandatory. Automated systems[7, 8] also exist that register who disposes of how much waste — a more detailed discussion of these can be found in 1.2.

More and more municipalities deploy some kind of measuring technology, however many of them choose not to differentiate the tariffs yet and use it only for monitoring and managing the waste flow.

## 1.2 Technologies

We've looked at the two main types of electronic waste registration: *shared* and *personal* containers. Both systems interface with a backend data processing system, as depicted below:

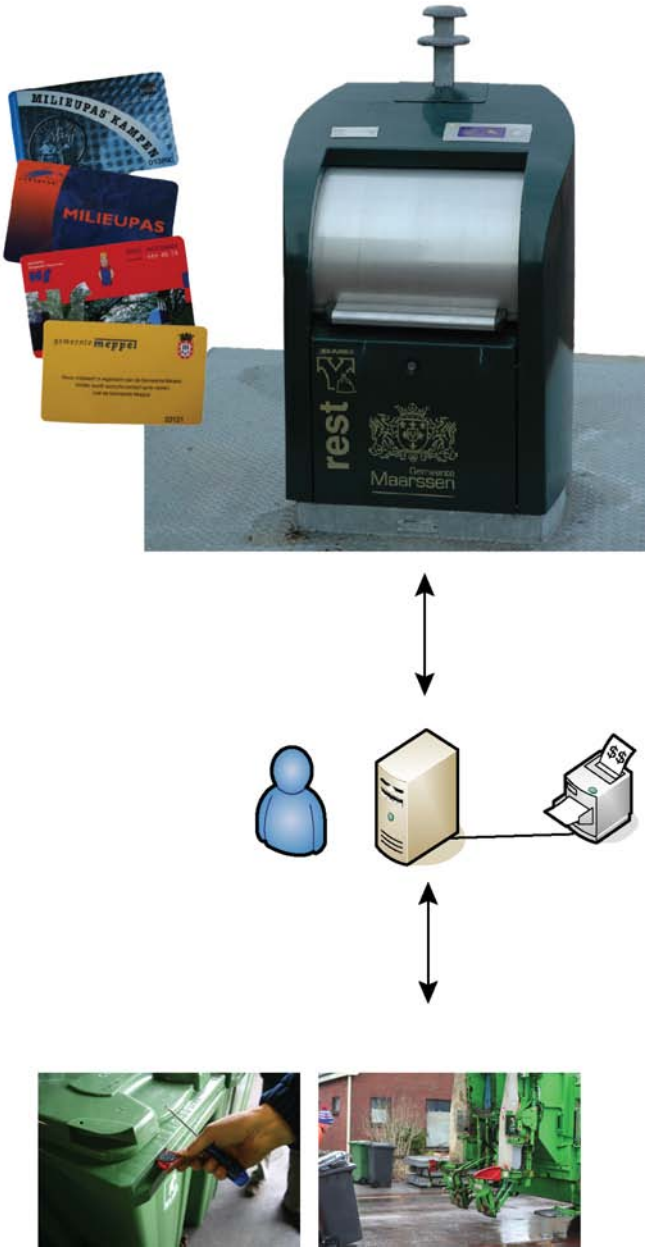


Figure 2: Overview

If the municipality is using diftar, then the data processing system will generate a tax bill based on the usage of either the shared container or personal container. Each technology will now be explained in more detail.

### 1.2.1 Shared containers

The first category is the shared underground waste container. Upon identification with an ID card people can dispose of their waste at any time in a nearby container. This system can also record how much waste each household has disposed of. It is usually found in more densely populated urban areas, where space restrictions may not allow for personal containers, or where it is desirable that people can dispose of their waste 24 hours a day. All shared container systems we encountered use a contactless ID card with radiofrequency identification (RFID) chip.

(a) Underground shared container

(b) Container arm swung aside, ready for emptying

(c) Valid ID card opens door

(d) Battery equipped GSM unit

Data is collected locally on a small computer and transmitted to a *data processing centre* or DPC. This can be done using several transmission techniques including GSM, GPRS, SMS, Mobitex and POTS. The container units can be powered by batteries, or they can be hooked up to the public electricity network.

### 1.2.2 Personal containers

The second category involves marking the domestic container of a household with an RFID-chip. The collection vehicle records this ID during emptying. The household might pay for each time the container is emptied; another scenario is to weigh the container and charge per weight unit. In the rest of this report we will use the term *personal container* to refer to this type of waste registration, although it is usually not bound to a discrete person but to a household. In general this strategy is employed in suburban and countryside areas, where people have room to store such containers.

(e) Personal container with identification tag

(f) Attaching and determining gross weight

(g) Emptying

(h) Determining tare weight

Data is accumulated on a small onboard computer and transmitted via the same wireless transmission techniques as the shared containers. Data can also be transferred manually using memory cards.

The DPC is usually run by a commercial collection company, or by the municipality itself and processes incoming data from collection vehicles or underground containers. It can be used to define which containers or access cards are permitted, to monitor environmental conditions of underground containers, or to keep track of internal waste levels of underground containers. This can then be used to plan more efficient routes for waste collection vehicles. The DPC typically aggregates collected data for management purposes, ultimately leading to invoices and tax bills for households.

## 1.3 Research focus

A variety of techniques are applied for identifying a household, registering the amount of waste disposed of, and communicating this data with the municipality. Currently at least WIFI, RFID and GPRS are used. Correct functioning of this equipment is pivotal. Households should not be able to evade the waste disposal costs or divert these costs to others. A disruption of the collection could have a serious impact on public life. However, as far as we know no previous research about the reliability and security of these systems has been available.

This research focuses on the following questions:

> What are the requirements for a good automated waste registration system for domestic collection?
>
> Which systems are available and do they meet these requirements?

## 1.4 Structure of this report

In this introduction we've defined and explained the concepts and processes in the context of this research, and defined the research questions. In chapter 2 we will lay the theoretical base of a secure system, which methods can be used to make a system secure, and define tests to measure the security of the systems that are the target of our research. This tries to answer the first of our two research questions.

Chapter 3 focusses on our second question and has the results of our research into the systems of a number of municipalities in the Netherlands, which we compare with each other and with the tests from the previous chapter. After that we will draw our conclusions and give some ideas for further research.

# 2 Theoretical background

## 2.1 CIA triad

The so-called CIA triad is generally accepted as the base of information security[9, 10, 11]. This triad defines three key concepts that provide the principles of a secure system — confidentiality, integrity and availability. It is often depicted as a triangle (see figure 3) to indicate that all three concepts are needed for complete security.


Figure 3: CIA triad

### 2.1.1 Confidentiality

A system that processes data must make sure that data can only be used, read or copied by parties (systems or persons) that are authorised to do so, and are only authorised when there is a genuine need for it. The confidentiality of a system is hence breached when an unauthorised person can access, use or copy data from the system.

Confidentiality is a necessary (but not sufficient) condition to protect the privacy of people whose data is collected by the system.

A number of things can lead to a breach of confidentiality:

- sending data over insecure connections
- storing data on insecure media
- viewing of data by unauthorised people
- deducting personal information from identification tokens

### 2.1.2 Integrity

Integrity denotes that key information on the system cannot be changed, created or deleted by persons or machines that are not authorised to do so. An additional requirement for integrity is that data stored in different subsystems are not in conflict with each other. This is closely related to the previous item: unauthorised persons should not be able to read information, and they should certainly not be able to change it. This is a key factor in making sure the data throughout the system will be the same as the originally measured data — thus preventing fraud, or accidental corruption of data. This is a very important property in cases where households are taxed on the basis of the information collected and processed by the system.

Integrity can be breached by:

- changing personal information
- changing measurement data
- identifying as someone else
- interrupting the synchronisation between subsystems

### 2.1.3 Availability

The third concept is the availability of a system, which means that the system to process the data and the security measures to protect the data are functioning correctly when they are needed. A system becoming unavailable could be caused by accidental damage (someone tripping over a power cord), or by a malicious person deliberately trying to break it.

Availability can be affected in several ways:

- physically breaking key components
- changing data in such ways that the system stops working
- interruption in the necessary infrastructure

## 2.2 Methods for keeping information secure

The CIA triad lays out the basic concepts that define system security. Given the confidentiality, integrity and availability requirements, we can define which methods and techniques are needed to realise these in the context of an automated waste registration system and in the subsystems *personal container*, *shared container* and *data processing centre* as defined in section 1.2. The subsystems are interconnected. The communication between data processing centre and waste collection vehicle, or between data processing centre and shared container, is regarded as being part of the data processing centre.

### 2.2.1 Confidentiality

The aim of confidentiality is to keep private that which doesn't need to be public. Automated waste collection systems collect data about an individual's behaviour: when they produce waste, how much they produce. Confidentiality is required to protect the privacy of person whose data is processed or stored by the system.

One may consider this data of relatively low value: the system stores who disposed of how much waste and when. However, the DPC may also contain more personal data about households like names, addresses and financial information.

Furthermore, it's generally desirable that a system does not leak information to those without a need to know.

The following measures can be taken to ensure confidentiality:

1. **Authentication**. The system should only give out information (read access) to entities that have successfully authenticated themselves. For personal containers, the ID chip contents may only be made available for reading when one has authenticated: the waste collector may have a secret that unlocks the data in the ID chip. For the underground container, the data processing system should identify itself to the container before it can read out the stored data. The user of the data processing system should be authenticated to prevent access by others.

2. **Authorisation**. For personal and shared containers, further authorisation is not necessary in the context of confidentiality: only authorised parties can authenticate themselves in the first place. The data processing system may use authorisation to discern classes of users, e.g. inhabitants that may read their own balance, and key users that can read all data.

3. **Cryptography**. An alternative to authentication + authorisation is to encrypt the data so it can only be read by an entity that is in possession of the secret used for encrypting that information. For personal containers that only carry an identification chip, this is not really relevant. The number itself is not sensitive information (cryptography can be used to make it harder to copy the number though, which is treated under *integrity*). Shared containers can encrypt the data they communicate with the DPC so eavesdroppers cannot read it.

Applicability of these techniques is summarised in the following table.

| | Pers. | Shared | DPC |
|---|---|---|---|
| Authentication | + | + | + |
| Authorisation | - | - | + |
| Cryptography | - | - | + |

### 2.2.2 Integrity

Integrity ensures that gathered information is authentic and has not been tampered with, preventing accidental loss and fraud.

Municipalities employing automated waste collection are basing decisions and operations on the data coming out of such systems, whether it is on a macro level (management and trends), a meso level (container filling levels), or micro level (taxing of individual disposals). It is in their interest, and that of the household that may receive a tax bill based on the system's data, that the data is reliable and accurate.

This may be the most important security property, especially when diftar is applied: people may be taxed for other people's garbage, without a convincing proof available to them that they didn't dump it.

To provide assurance of integrity the following measures can be taken:

1. **Authentication**. Write access to the system should only be allowed to entities that can be authenticated first. Regarding personal containers, successful authentication means a container is identified and hence can be registered as a valid disposal. For the shared container, authentication ensures that it's known who disposes of a load, so again who can be taxed. The data processing system must allow only the administrator to insert, update and delete data.
2. **Authorisation**. Authorisation to protect integrity can be used on both personal and shared containers when working with white and black lists to specify if a given container or card ID is allowed.
3. **Cryptography**, including checksums. To make unauthorised creation of a valid container more difficult, cryptography can be used on personal containers to ensure uniqueness of an identification chip, or with shared containers of the ID card. The data processing system and the shared container can use checksums to ensure data does not get accidentally corrupted in transit, or cryptographic signing with a key created by the municipality to protect data from being tampered with.
4. **Logging** and monitoring. Every part of the system can log all events, including failures and unexpected events, to make it possible to detect a breach of integrity even if it could not have been prevented. Invalid ID chips on personal containers, invalid ID cards, and other anomalies can be flagged by the data processing system. Part of this is rate limiting on user access, so any compromised authentication has only limited consequences.

To summarise the applicability of above items:

| | Pers. | Shared | DPC |
|---|---|---|---|
| Authentication | + | + | + |
| Authorisation | + | + | + |
| Cryptography | + | + | + |
| Logging | + | + | + |

### 2.2.3 Availability

Availability ensures that a system can actually be used for its intended purpose. That this is important can be seen in the cited examples in the introduction: when waste collection stops, the consequences for a society can be anywhere from inconvenience to chaos.

To facilitate availability, the following measures can be taken:

1. **Physical security**. A low tech way to stop a system from working is to physically approach it and disable it. Especially for the data processing system good physical security is important. For personal containers this is unfeasible because they have to be put out on the street anyway. For shared containers there can only be very limited physical security provided by the casing.

2. **Rate limiting**. A system can be made unavailable by overloading it. This is not relevant for personal containers, because these only contain an ID chip, and if it would be possible to overload it, the scope is just the container itself. With shared containers one could for instance try to drain the battery. If the data processing system is reachable through a public network, a remote *denial of service* or DoS attack is possible. Rate limiting can stop or slow down requests when the load reaches a certain threshold. The impact of this may be low, because the DPC does not need to be up for the rest of waste collection to remain functional.

| | Pers. | Shared | DPC |
|---|---|---|---|
| Physical | - | +/- | + |
| Rate limit | - | + | +/- |

## 2.3 Practical implications

Based on the demands of a secure system put forward by the CIA-model as discussed in sections 2.1 and 2.2, we can derive the practical demands that this has for an automated waste registration system. Checkmarks indicate whether or not a test applies to a collection strategy.

### 2.3.1 Confidentiality

1. **Authentication** – Data should not be accessible without identification.

| | | Pers. | Shared | DPC |
|---|---|---|---|---|
| A. | DPC requires authentication? | - | - | ✓ |
| B. | Reading RFID tags requires authentication? | ✓ | ✓ | - |
| C. | Reading from shared containers requires authentication? | - | - | ✓ |

2. **Authorisation** – Closely related to authentication, but defines who can read what.

| | | Pers. | Shared | DPC |
|---|---|---|---|---|
| A. | Can users see other user's data? | - | - | ✓ |

3. **Cryptography** – Can be used to protect communication to and from the data processing centre, which might include physical media like memory cards that are used to transfer data to and from a collection vehicle. This can be considered as communication between data processing centre and personal containers (considered in this report to be the domain of the DPC). We also take into account an end user not using the DPC directly, but via an extra channel. This seems to be rather common, for instance if the DPC is hosted externally, and can be used online.

| | | Pers. | Shared | DPC |
|---|---|---|---|---|
| A. | Is communication with end user encrypted? | - | - | ✓ |
| B. | Is communication with shared container encrypted? | - | - | ✓ |
| C. | Are physically transferred media encrypted? | - | - | ✓ |

### 2.3.2 Integrity

1. **Authentication**

| | | Personal | Shared | DPC |
|---|---|---|---|---|
| A. | DPC uses authentication for altering data? | - | - | ✓ |
| B. | Will a container without ID be emptied? | ✓ | - | - |

2. **Authorisation**

| | | Personal | Shared | DPC |
|---|---|---|---|---|
| A. | Can users of the DPC only alter the data they're entitled to? | - | - | ✓ |
| B. | Will an unknown ID get emptied/accepted? | ✓ | ✓ | - |
| C. | Can IDs be blacklisted? | ✓ | ✓ | - |

3. **Crypto/checksum** – mostly the same as authentication, but this deals with prevention of writing/changing/deleting of data.

| | | Personal | Shared | DPC |
|---|---|---|---|---|
| A. | Does the DPC use encryption in its communication? | - | - | ✓ |
| B. | Do RFID tags give out ciphertext? | ✓ | ✓ | - |
| C. | Are data batches from shared containers signed? | - | - | ✓ |

4. **Logging/monitoring** This is used to enable detection and recovery from any breach in the system integrity. User rate limiting means that a household is limited to depositing a maximum reasonable amount per day, to limit the damage in the case of compromise.

| | | Personal | Shared | DPC |
|---|---|---|---|---|
| A. | Does the DPC log all events? | - | - | ✓ |
| B. | Are all scanned IDs logged? | ✓ | ✓ | - |
| C. | Are users rate limited? | ✓ | ✓ | - |

### 2.3.3 Availability

1. **Physical security**. We will not look at the DPC's physical security because that is outside the scope of this research project. Physical security of personal containers is not feasible because they need to be put out on the street anyway. Hence this only applies to the shared containers.

| | | Personal | Shared | DPC |
|---|---|---|---|---|
| A. | Possible to disrupt power supply? | - | ✓ | - |
| B. | Possible to disrupt communications? | - | ✓ | - |

2. **Rate limiting**. This deals with several flavours of *denial of service* attacks. Not applicable to personal containers.

| | | Personal | Shared | DPC |
|---|---|---|---|---|
| A. | Is it possible to conduct a DoS attack? | - | ✓ | ✓ |

# 3 Results

In section 2.3 we defined a number of concrete requirements for waste collection systems. In this chapter we will discuss our findings of different systems in use around The Netherlands. They will be sorted by collection strategy. Many municipalities use multiple strategies in parallel.

Our main findings will be shown in matrix form where we give the results of our tests of the requirements from section 2.3. After each matrix the text will go into detail on the system and why we arrived at the conclusions in the table.

## 3.1 Personal Containers

| | | Oostzaan | Kampen | Meppel | Hoogezand | Apeldoorn |
|---|---|---|---|---|---|---|
| | diftar? | yes | yes | no | yes | yes |
| C1B | reading requires auth? | ? | no | ? | ? | ? |
| I1B | tagless bin emptied? | yes | no | no | no | no |
| I2B | unknown tag emptied? | yes | yes | no | yes | no |
| I2C | can blacklist tags? | yes | yes | yes | yes | yes |
| I3B | is tag crypted? | ? | ? | ? | ? | ? |
| I4B | logging of events? | yes | yes | yes | yes | yes |
| I4C | rate limiting? | no | no | no | no | yes |

### 3.1.1 Oostzaan

The municipality of Oostzaan (province Noord-Holland), with 4000 households, was the first in the Netherlands to implement diftar in the early nineties[12]. It works with personal containers and a tagging system by Jama BV[19]. The containers are weighed and the number of kilos is registered on a memory card in the vehicle. This process can be seen on page 1.2.2. The memory card is read in at the municipal office. Duplicate or unknown containers are signalled during emptying, a note is made of the exact location and physical number of the container, after which it is accepted for emptying. Each of the encountered anomalies has to be checked by hand afterwards, and in-person action is taken when suspicion is raised. The relatively small size of the town allows for this to work effectively.

The identification chip used is supplied by Nedap[22], which uses a proprietary and secret protocol. The documentation suggests that it gives out a single ID without further authentication, but that is not sure. We have not been able to find out more about this tag yet.

### 3.1.2 Kampen

Kampen (province Overijssel) is a town with around 20 thousand households. They use both shared and personal containers to implement diftar[13]. The system is provided by WSS InfoCard Systems BV[20]. Households pay a fixed amount for every time they offer their bin for collection. The vehicle is equipped with a palmtop computer that has a blacklist of unacceptable containers. A container without tag is not accepted at all, an unknown one will be emptied but added to the blacklist as soon as the data is analysed at the municipal office. This allows to offer an unknown container for a short while. When a container is encountered for the second time in a round it is charged for the second time. Every event is logged, including scan errors and rejected containers. Anomalies are acted upon when required.

The tags in the containers are of the EM 4x50 type[24]. An example of the output of such a tag can be found in A.1. The tag can be read out entirely with a standard ACG Low Frequency

reader, except for the first sector which may contain a password. This password and the feature allowing tags to be writable are not used in Kampen.

Because all relevant data can be read out entirely, making a clone should be possible. We did not have blank tags of this type however, so this was not tested in practice. Because containers are not refused when encountered a second time in a round, creating a clone of an existing container in another street (which are outside all day) is a feasible way of rerouting charges to someone else. The tags have the feature of setting a password required to read the tag's contents; however, the system does not use this feature.

We have not yet deciphered the relationship between the data on the tag and the ID that is registered by the vehicle, so creating a new valid ID out of an existing one is not possible by us in a straightforward way.

### 3.1.3 Meppel

The town of Meppel (province Drenthe) has over 13 thousand households. It does not employ diftar, but uses automated waste registration for monitoring and control purposes[14]. The system for tracking personal containers is supplied by WSS InfoCard Systems BV [20]. It is very comparable to the system in Kampen, with the notable exception that no taxing is done.

### 3.1.4 Hoogezand-Sappemeer

Hoogezand-Sappemeer (province Groningen) has around 17 thousand households. For diftar it uses both shared containers and personal containers[15]. Containers without ID are refused during collection, but since the system works with a blacklist, an unknown ID will be emptied initially. However, during processing at the municipal office this will be noticed and the container will be added to the blacklist for the next round of collection. The system is largely the same as in Meppel, see there for more details.

### 3.1.5 Apeldoorn

In Apeldoorn (province Gelderland) with 66 thousand households, Circulus BV is responsible for the collection of waste on behalf of the municipality. It too employs a diftar system[16] with personal and shared containers, and a separate system for a visit to the central waste separation station. Households pay for every time their container is emptied. The system has been developed to fit into Circulus's Aris waste management system and uses ID chips supplied by Jama BV of the same type as encountered in Oostzaan.

The waste collection vehicle works with a whitelist, so unknown ID's or containers without ID are not emptied at all. Data exchange between vehicle and office (collection data and white-list) is updated via GSM. This also allows the removal of a stolen container from the white-list while the vehicle is *en route*. Duplicate containers are not accepted for the second time in a round, which means that a duplicate will be quickly detected. The driver of the vehicle can not override this restriction nor the white-list.

## 3.2 Shared Containers

| | | Hoofddorp | Kampen | Meppel | Hoogezand | Apeldoorn |
|---|---|---|---|---|---|---|
| | diftar? | no | yes | no | yes | yes |
| C1B | auth to read tag? | no | no | no | no | ? |
| I2B | unknown tag works? | yes | no | no | no | no |
| I2C | can blacklist tag? | no | yes | yes | yes | yes |
| I3B | crypted tag? | no | yes | yes | yes | yes |
| I4B | all tags logged? | ? | ? | ? | ? | ? |
| I4C | rate limiting? | no | no | no | no | no |
| A1A | disrupt power? | yes | no | yes | no/yes | no |
| A1B | disrupt comms? | - | no | no | yes | no |
| A2A | DoS? | no | yes | no | yes | no |

### 3.2.1 Hoofddorp

Hoofddorp (province Noord-Holland) is a fast growing town of the municipality Haarlemmermeer, which has around 55 thousand households. It does not employ diftar yet, but its newly developed neighbourhood 'Floriande' is equipped with underground shared containers, which need to be opened with a key card. According to the municipality this is purely access control, there are no further limits or taxes on the amount of use. The system is supplied by Diftar BV.

The cards in use are RFID's of the EM 4x02 type[23]. A sample of such a card can be found in A.2. All this chip does is to produce an ID which can be read out. By using the ACG low frequency (125 kHz) RFID reader/writer and the RFIDIOt software[26], we could make a clone of this card in a matter of seconds, with which we could open any container we tried. When we started generating cards with other ID numbers, it turned out that any card we made would open the containers, for example: `0000000001`, `1000000000` or `FFFFFFFFFF` with one notable exception: a card returning all zeros does not work. This may be an ID of a special card, or just a limitation of the used software.

This means that probably every EM 4x02 type card can open an underground container in Hoofddorp. Additionally we tested for rate limiting on these containers, and succeeded in making at least 50 deposits each with two different cards.

According to the municipality the system does not communicate with a central data processing system. It runs on a battery, which may be emptied, especially in the light of many subsequent transactions being possible without any charge.

We were not the first ones to find out about this. In August 2007, someone offered to replace a lost card for a price much lower than the replacement cost charged by the municipality[6].

### 3.2.2 Kampen

Next to personal containers, Kampen also employs shared containers in some neighbourhoods. Households pay for every bag of waste deposited. The first generation was supplied by Kliko BV, and Kampen is now in a trial with two new suppliers. The software is supplied by WSS InfoCard Systems. These containers are connected through the standard 230V mains and a standard phone line. This will be changed to batteries and GSM in the near future, because of the complications of wired connections in terms of cost and administration.

The containers accept an unlimited number of deposits by a single user per day. The ID card used for accessing the container employs the same EM 4x50 technology as used in shared containers. A read-out of such a card can be found in A.1. For more details about this chip, see the section on shared containers, 3.1.2.

### 3.2.3 Meppel

Meppel has introduced underground containers initially for business waste, but has extended this to households as well. Volume contracts have been made with businesses, disposal for households is not differentiated. The system in use has been supplied by Diftar BV.

Access to the container is gained by using an EM 4x02 style card with a unique ID (the same system as in Hoofddorp), for an example see A.3. A notable difference from Hoofddorp is that here a household is assigned a specific container for its waste: each container has a white-list with accepted households. This makes it harder to create a valid ID that will work on a specific container. It is still easy to clone an existing pass. Because there is no charge for specific waste, the consequences of this for an inhabitant may be small.

The containers get their power from a battery and are connected through GSM. A white-list of acceptable caller ID's, which is kept secret, and a proprietary communications protocol are used to make unauthorised access hard. The data transfer is protected against corruption through a checksum, and encrypted with a key that includes the container's phone number and location. Deposits have a sequence number to detect missing data. Because also commercial entities with many bags per day also use the containers, any ID may deposit an unlimited number of times per day.

### 3.2.4 Hoogezand-Sappemeer

Hoogezand-Sappemeer uses a system of underground shared containers. The first generation is supplied by Diftar BV, the second by Mic-O-Data BV. Households pay per deposit made. The Diftar systems use the Mobitex network to communicate with a central receiver at the municipal office, which reports back on successful receipt. The Mic-O-Data containers use SMS to exchange their data with Mic-O-Data's server (once a day), which then supplies it through a web interface to the municipal office.

The ID cards used to access the underground containers are EM 4x02's with a unique ID, in a similar fashion as in Meppel: a white-list of who can dispose in each container. See above for more details on this type of card. Appendix A.4 has an example ID card.

A crucial difference from Meppel is that Hoogezand-Sappemeer charges inhabitants per deposit, so the clonability of this card has material consequences. A possible scenario to exploit this would be for one to borrow the card of a neighbour "for just one deposit", and to quickly clone it. If the attacker does this with several neighbours it can easily go unnoticed. Alternatively it's relatively straightforward to skim the contents of the (contactless) card at the underground container itself.

Power to these underground containers is supplied through induction via a nearby 230V mains connection for the Diftar BV containers. This cannot easily be sabotaged except by putting a large metal plate between the power source and container, which in our opinion is not very feasible on a larger scale. The Mic-O-Data containers use a battery that could in theory be emptied. There is no limit on the number of deposits anyone can do in a given time frame.

### 3.2.5 Apeldoorn

Next to the personal containers, Circulus BV in Apeldoorn also uses shared containers. The system on these containers has been developed specifically for them to integrate with their waste management system Aris. The registration system was acquired from Vconsyst[21]. According to Vconsyst the system uses 134 kHz RFID cards from Texas Instruments. Our research into available types that match the physical specifications suggests that this is most probably the RI-TRP-R4FF or RI-TRP-W4FF[25].

The containers are connected to a regular mains power supply and data is exchanged over regular phone lines once a day to exchange deposits and white-lists.

We received a sample ID card but were not able to read anything from it. This needs further research, because based on the specs of this tag and our reader it *should* be readable. We've sent this tag to Adam Laurie of The Bunker Ltd.[26] for further analysis with a native Texas Instruments reader.

Households are not limited in the amount of deposited bags per day.

## 3.3 Data Processing System

| | | Oostzaan | Kampen | Meppel | Hoogezand | Apeldoorn |
|---|---|---|---|---|---|---|
| | diftar? | yes | yes | no | yes | yes |
| C1A | requires read auth? | yes | yes | yes | yes | yes |
| C1C | shared requires read auth? | yes | yes | yes | yes | yes |
| C2A | can see user data? | no | no | no | no | no |
| C3A/I3A | comm user crypted? | - | - | no | no | - |
| C3B/I3A | comm shared crypted? | - | ? | no | ? | ? |
| C3C/I3A | media crypted? | no | no | no | no | no |
| I1A/I2A | requires write auth? | yes | yes | yes | yes | yes |
| I3C | data signed? | no | no | no | no | ? |
| I4A | uses logging? | yes | yes | yes | yes | ? |
| A2A | can be DoSsed? | no | no | yes | no | no |

### 3.3.1 Oostzaan

In Oostzaan the data processing centre is a fully off-line system. Data is collected on a 512 kB memory card in the waste collection vehicle, in plain text lines with date, time, chip number and weight. The memory card is brought to the municipal office. An employee has to manually check every anomaly (unknown container, duplicate container, etc) and resolve this before the data can be sent to the finance department. After processing all entries, an updated blacklist can be written to the memory card and it is returned to the vehicle.

A household will receive a tax bill with a full specification of all emptyings and kilograms, which they can check. The system runs on an office computer and does not have any external interfaces.

### 3.3.2 Kampen

Data transfer between the waste collection vehicle and the data processing system currently happens by transferring the hand-held onboard computer, which contains plain ASCII data files with date, time and chip number (EAN). A new wireless transmission system over WiFi is currently being trialled. Our tests revealed that this wireless connection is encrypted with Wired Equivalent Privacy[17]. WEP is known to have fundamental security problems[18], making it crackable within minutes. The data that is transferred has a very straightforward format, which could make changing it in transit feasible. We have not yet tested this in practice though.

For the communication with underground containers, a modem dials these regularly to collect data and updates white-list. This is currently once every three days, so a rogue or stolen card cannot be blocked very fast, but individuals are indemnified by the municipality against any cost charged on their lost card from the moment they reported it as missing. Kampen does not use the filling level monitoring to plan its routes because it proved not reliable enough, but rather use its own experience.

### 3.3.3 Meppel

The data processing system in Meppel is split between the two ways of collecting waste: personal and shared containers. The data from personal containers is collected through a similar system as in Kampen, from the same supplier. Data is collected on a memory card and read in at a local work station, processed, and delivered to the financial department.

For the underground containers, they use a web-based application, WebWaste, which is fully developed and hosted by Diftar BV. The municipality logs in over the internet on this web application.

The online system does not store personal information from any inhabitants, but does allow to viewing and alteration of addresses, chipcard numbers, black- and white-lists. Additionally the filling rates of containers can be viewed.

Logging in is not encrypted (plain HTTP), and the system is reachable from any location in the world. This allows for sniffing the login credentials or remotely brute forcing them or executing a denial of service attack. All data is stored on the hosted server at Diftar BV, the municipality does not have control over the collected data.

### 3.3.4 Hoogezand-Sappemeer

The data processing system used by Hoogezand-Sappemeer is split up over the two collection methods. The personal container data is collected in CardView, also developed by Jama BV and the same application as used in e.g. Oostzaan. Special software has been developed that interfaces the system from the underground containers by both Diftar BV (Mobitex) and Mic-O-Data (web interface) with their waste management application Prevent.

The Mobitex system is a closed communications system also in use by e.g. emergency services. Through the use of a private APN, eavesdropping is hard. It is always online, delivering the waste disposal data directly as it happens, reducing the time window to interfere with it. The SMS-based system from Mic-O-Data is similar in the sense of being realtime, but is more public and a message may get lost in transit. It is unknown to us how easy it would be to send a forged SMS to this system.

The data gathered by Mic-O-Data is provided to the municipality over a web interface, i.e. over the public Internet. Unfortunately access to this system is not encrypted (plain HTTP), both for logging in and for the actual data being sent, making it possible to listen in on authentication credentials or the exchanged data.

Collection data is sent to the financial department which takes care of invoicing the inhabitants. The exact list of emptyings is included with the tax invoice.

### 3.3.5 Apeldoorn

Communication between the Apeldoorn system and the containers or vehicles happens over GSM. The waste collection vehicles can even be updated while in transit, for example to add new entries to the blacklist.

The data processing system itself is a custom application developed to fit in with their waste management system Aris. It runs locally on a computer at Circulus BV.

Unfortunately we haven't found out more about this system yet.

# 4 Summary

## 4.1 Findings

At the beginning of this four-week research project there was not much information available about the security aspects of electronic waste registration. The only information came from vendor websites, and turned out to be both biased and too non-technical. Therefore we had to start from scratch and make an inventory of what was actually used in the real world. This involved visiting several sites around the country, doing experiments, interviewing civil servants, sales people, and developers.

Every municipality has its own needs. Combined with the fact that there are several vendors and several generations of technologies this results in a matrix of different systems being used in the field: we saw a lot of variation in waste containers, waste collection vehicles, RFID tag types, communication setups, and DPC's, while the essential problem they try to solve is very similar.

We did not find evidence that the security of electronic waste registration systems had been taken into account by municipalities when posing the requirements of such a system, although in some situations systems have been in place for more than 15 years, making it difficult to find the responsible persons.

Relatively simple RFID's such as the EM 4x02 can be cloned very easily. Using them as an identifier in situations where money is involved, such as electronic waste registration, is a security risk. Cloning the ID of a personal container will in some cases raise alarms during data processing, so there the risk is limited.

Cloning an ID card for a shared container can have more effects. Multiple transactions are normal, so abuse would not immediately be noticed. Cloning the ID card requires the original ID card, but this could be done in various ways: borrowing ID cards, or skimming them. If an attacker knows details about the numbering scheme he could also use enumeration attacks. However, most shared containers use a white list so only a limited set of ID cards can be used. An interesting issue in this respect is the existence of maintenance cards, which can be used to open any container in a municipality. Cloning such a card means disposing of waste without paying. It is likely that these cards are used by vendors too. This means that in the event that a maintenance card is abused it will have to be removed from all white lists in all municipalities, and that all vendor employees would have to change their maintenance cards. Therefore these maintenance cards can be considered as the 'holy grail' for attackers.

If we do not take the proprietary RFID tags into account, we did not find any tags that used a password, login procedure, or encryption, despite the fact that at least one tag (the EM4x50 in personal containers in Kampen) was capable of protecting read actions.

Recently, in 2006, the Comité Européen de Normalisation (CEN) has defined a standard in this area: NEN-EN 14803: Identification and/or determination of the quantity of waste[27]. Apart from physical characteristics, this standard determines one format for the ID of personal containers. Section 4.6.1.1 defines that all tags must be publically readable, without encoding or encryption. This is exactly what makes these tags easy to duplicate, which makes it an unfortunate requirement. We believe that encryption, when well-defined, does not make a system less exchangeable.

The backend data processing systems are mostly relatively secure because they run on a computer inside the municipal office. However, we saw a case where the wireless connection between vehicle and office was protected via WEP. Also the systems hosted through an application service provider model did not use SSL to encrypt traffic over the internet. This shows a lack of awareness of very basic measures to secure connections.

The root cause of these problems may be that there is not much knowledge nor concern about security among municipalities while implementing electronic waste registration. Because security

is not part of the demands, or cannot be properly judged or evaluated by the civil servants, security doesn't get too much attention from the companies that sell these systems.

## 4.2 Conclusion

Reviewing our research questions from section 1.3:

> What are the requirements for a good automated waste registration system for domestic collection?

To answer this question, we have defined tests based on the three cornerstones of information security: confidentiality, integrity and availability, specifically to automated waste registration in chapter 2. An ideal system will not compromise on any of these aspects, but practical demands often make compromise necessary. In our specific situation, a breach of confidentiality may be undesired, but in most cases the processed information is of relatively low value: who has deposited which quantity of waste, and when. A problem with availability can in the worst case lead to chaotic scenarios, but in many cases the municipality can just return to old-style non-differentiated collection. In the context of this research, integrity is the most important quality. As soon as money is involved it will become profitable to subvert the system. A breach of integrity can also degrade the public's trust in the system that is used to tax them. Insufficient safeguards for integrity may open up the possibility of claims from households that challenge the cost they are charged, without convincing evidence that they did in fact deposit that amount of waste.

> Which systems are available and do they meet these requirements?

We found many different systems or combinations, and expect that further research will uncover even more. Chapter 3 gives an overview of these and also matches each up with the requirements we put. We can see that although some tests are matched by many of the systems, no system scores well on (nearly) all tests. Especially in the area of integrity, which we rate as most important, these systems leave ample room for improvement.

The implications of the problems we found seem few when a municipality does not use diftar. For example the Hoofddorp case, where any card can open any container, does not have many implications for the inhabitants, except that it defies the reason why access control was implemented in the first place. However, all of the 'non-paying' municipalities are at least investigating the possibility of introducing diftar. It is doubtful that they will then switch to a completely different system.

# 5 Recommendations

Based on our findings, we make the following recommendations when implementing an automated waste registration system. We recommend the following concrete technological measures.

**RFID tags should be secured against readout.** Cards like the EM 4x02 series that present only a single ID can be easily cloned or enumerated. This risk is increased by the fact that no physical contact is needed to read them out. Tags exist that require a secret before they reveal their information (like the EM 4x50), this prevents unauthorised generation of a fake ID. This includes updating NEN-EN 14803 4.6.1.1 to reflect this.

**Whitelists should be used rather than blacklists.** Even if a tag can be constructed, when the containers use whitelists of acceptable IDs, the usefulness of an unauthorised tag is much smaller. Also for personal containers, the vehicle can proactively store which bins are valid instead of reactively disable rogue bins.

**Use rate limiting to control abuse.** If a personal container is only accepted once per collection round, the use of a clone gets noticed instantly. Similarly, underground containers should pose an upper limit on what is reasonable to dispose of, to prevent unlimited malicious transactions. In the latter case it may be complicated to cope with households that have temporarily a lot of waste (e.g. when moving house).

**Access to backend systems should be appropriately restricted.** The web based management systems we found did not employ SSL encryption of logins, which can be considered a basic requirement of every web application. They are reachable from the entire internet, while there are at most only one or two workplaces that need to use it.

**Every unexpected event should be monitored.** Even if the system is not watertight in a technical sense, monitoring and following up on every unexpected event makes a system resistant to abuse, especially in smaller communities.

**Households should have insight into the individual transactions on their account.** In order to detect malicious use, a household should be able to easily verify the transactions attributed to it. This also helps to improve the transparency of the taxed amounts.

**The market should consolidate to less but better solutions.** The current demand for diftar systems is small, but the number of different systems is large (even within a single supplier), each solution being problematic in one way or the other. Instead it would be better for the market to converge into just a few parties that each offer one well-tested solution.

The following recommendations apply to and are confirmed by the problems found in this research but could also be more generally applied to enhance the security of public ICT projects.

**Obscurity is not sufficient for a secure system.** If the system depends on obscurity of its methods, especially with very public systems like waste registration, someone is sooner or later going to find out how it works. Instead, rely on methods that work even if widely published (Kerckhoffs' principle[28]).

**Encryption is here to help.** A lot of research has gone into developing strong cryptographic algorithms, yet the systems we have seen hardly employ any to ensure the confidentiality or integrity of data. ID cards, bin tags, data storage, data communication and authentication could all have been much better secured using publically available encryption and signing methods.

**Security demands should be part of selection criteria.** We have not encountered municipalities making concrete demands on their suppliers on the security of diftar systems they implement or operate. Suppliers are not going the extra mile for security if there's no demand from customers.

**Public projects should have public security evaluations.** For projects that are funded with public money and serve a public cause, the implementation details should be similarly public, so that every individual affected by it can verify the integrity of such a system. This way developers are forced to properly implement security measures.

### 5.1 Future research

The lack of prior research into the technical aspects of automated waste registration and the limited time available, forced us to give more of an overview rather than to go in-depth on specific technologies.

Our research is just a sample. A more comprehensive survey could be made of all municipalities that use automated waste registration, which will no doubt reveal even more different systems in use.

Further research in the area of RFID could concentrate on investigating one specific tag more deeply, for example the Nedap proprietary ID's, the for us unreadable Texas Instruments ID or decoding the data sent out by the EM 4x50 tags.

Another approach could be to examine an underground container setup and investigate concrete ways to insert, modify or delete data on such a container or in the communication with the data processing centre.

Lastly more research is welcome into the reasons why security is not high on the agenda in this part of the public sector, and how that could be changed.

## 6 Thanks

While conducting this research project, we received the generous help from the following people, to whom we would like to express our gratitude for their information, guidance, explanation, tours and demonstrations.

Ingrid Rabe (Gemeente Oostzaan), Eimert Boerman and Joop Snoeijer (Gemeente Kampen), Wim Hilberink (Gemeente Meppel), Klaas Bouwknecht (Gemeente Hoogezand-Sappemeer), Edwin Veenhuizen (Circulus BV), René Jongejans (LoadIT BV), Egon Honingh (Diftar BV), Marten van Marle (JAMA BV), Jorus Kalter (Vconsyst BV), Thierry van Zandvoort (WSS Infocard Systems BV), Adam Laurie (The Bunker Ltd.), dr Rudy Negenborn (TU Delft), Jeroen van Beek, Marc Smeets and Hans IJkel (KPMG).

# References


[1] *Garbage Crisis Stirs Protest in Naples.* Associated Press, 4 January 2008. `http://ap.google.com/article/ALeqM5iHdYGgFyVTKkhbtHxQWZR0y12g0wD8TVE46O1`

[2] *Sail bedreigd door tonnen aan huisvuil.* De Volkskrant, page 2, 15 August 2005.

[3] Centraal Bureau voor de Statistiek, *Gemeentelijke afvalstoffen; hoeveelheden.* CBS StatLine, `http://statline.cbs.nl/StatWeb/Download.asp?LYR=G1:0&LA=nl&DM=SLNL&PA=7467&D1=0-3,5-9,73&D2=0,5-16&D3=a&STB=T&HDR=G2&TT=2` (source data in English: `http://statline.cbs.nl/StatWeb/Table.asp?PA=7467eng&D1=0-163&D2=0&D3=a&DM=SLEN&LA=en&TT=2`)

[4] Centraal Bureau voor de Statistiek, *Gescheiden afvalinzameling stagneert.* CBS Webmagazine, 18 July 2007.

[5] Didde R., *Afvalchipknips en stofzuigersystemen: de combinatie van ondergrondse afvalinzameling en diftar maakt school.* Milieumagazine vol 13 nr 3, page 10–13, 2002.

[6] *Fraude met pasjes van containers Floriande; Gemeente doet aangifte tegen clandestiene verkoop.* Haarlems Dagblad ed. Haarlemmermeer, page 201, 22 August 2007.

[7] Fuhrer P. et al., *RFID: From Concepts to Concrete Implementation.* IPSI-2006 Marbella, 2006.

[8] Engberg S.J. et al., *Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience.* Second Annual Conference on Privacy, Security, and Trust, 2004.

[9] Pfleeger C.F., *Security in Computing.* Prentice Hall, 1989.

[10] Russell D., *Computer Security Basics.* O'Reilly, 1991.

[11] International Organisation for Standardisation ISO: *ISO/IEC 27002: Code of practice for information security management.* NEN-ISO/IEC, 2005.

[12] Linderhof, V., Kooreman, P., Allers, M., Wiersma, D., *Weight-based pricing in the collection of household waste: the Oostzaan case.* Resource and Energy Economics 23, page 359–371, 2001.

[13] *Hoge diftar-idealen van destijds moeten nu noodlanding maken.* De Stentor/Nieuw Kamper Dagblad, page 2, 12 November 2003.

[14] *Afvalcontainers ondergronds in Meppel.* Apeldoornse Courant, 27 March 2003.

[15] *Plan om ook kunststof uit afval te halen; Onderzoek gemeente Hoogezand-Sappemeer.* Dagblad van het Noorden, 1 October 2007.

[16] Van Raffe, J.K. and De Boer, T.A., *Afvaldumping in de natuur.* Alterra rapport 1530, 2007.

[17] Institute of Electrical and Electronics Engineers, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* ANSI/IEEE Std 802.11, 1999.

[18] Borisov N., Goldberg I., Wagner D., *Intercepting Mobile Communications: The Insecurity of 802.11.* Proceedings of the Seventh Annual International Conference on Mobile Computing And Networking, ACM, 2001.

[19] Jama BV, *JAMA Diftar Applicaties.* `http://www.jama.nl/nl/systems/diftar.htm`

[20] WSS InfoCard Systems BV, *Diftar voor ondergrondse en bovengrondse containers*. http://www.wssnl.com/

[21] Vconsyst, *Vconsyst toegang en registratie*. http://www.vconsyst.nl/default.aspx?cid=14&nid=66

[22] Nedap Industrial Identification, *RFID transponders Product Bulletin*. http://www.nedapindustrialid.com/downloads/eng/Transponders_ProdBull_v2.2_E.pdf

[23] EM Microelectronic-Marin SA, *EM4102 Read Only Contactless Identification Device*. http://www.emmicroelectronic.com/webfiles/Product/RFID/DS/EM4102_DS.pdf

[24] EM Microelectronic-Marin SA, *EM4450 1 KBit Read/Write Contactless Identification Device*. http://www.emmicroelectronic.com/webfiles/Product/RFID/DS/EM4450_DS.pdf

[25] Texas Instruments, *RI-TRP-R4FF, RI-TRP-W4FF Card Transponder*. http://focus.ti.com/lit/ds/symlink/ri-trp-w4ff.pdf

[26] Laurie, A., *RFID IO tools*, http://www.rfidiot.org/

[27] Comité Européen de Normalisation, *NEN-EN 14803: Identification and/or determination of the quantity of waste*. NEN-EN, 2006.

[28] Kerckhoffs, A., *La cryptographie militaire*. J Sci Militaires, nr 9, page 5 – 38, 1883.

# A RFID contents

## A.1 Kampen

### Personal Container

```
readlfx v0.1k (using RFIDIOt v0.1r)
  Reader: ACG LFX 1.0  (serial no: 08070045)
Card ID: T8A9E0500
Tag type: EM 4x50

 sector 00:  Read error X
 sector 01:  00000000
 sector 02:  1C200100

 sector 03:  00000000
 sector 04:  87E09DD8
 sector 05:  93C58505
 sector 06:  1054B22E
 sector 07:  31BDBE72
 sector 08:  00000000
 sector 09:  00000000
 sector 0a:  00000000
 sector 0b:  00000000
 sector 0c:  00000000
 sector 0d:  00000000
 sector 0e:  00000000
 sector 0f:  00000000

 sector 10:  00000000
 sector 11:  00000000
 sector 12:  00000000
 sector 13:  00000000
 sector 14:  00000000
 sector 15:  00000000
 sector 16:  00000000
 sector 17:  00000000
 sector 18:  00000000
 sector 19:  00000000
 sector 1a:  00000000
 sector 1b:  00000000
 sector 1c:  A7E92730
 sector 1d:  CB987ADA
 sector 1e:  19BB4194
 sector 1f:  66A0A0D3

 sector 20:  8A9E0500
 sector 21:  32100011
```

**Shared Container ID card**


```
readlfx v0.1k (using RFIDIOt v0.1r)
  Reader: ACG LFX 1.0  (serial no: 08070045)
Card ID: T309C2800
Tag type: EM 4x50

 sector 00:  Read error X
 sector 01:  00000000
 sector 02:  1C200100

 sector 03:  00000000
 sector 04:  87BBFB00
 sector 05:  9383BD02
 sector 06:  63D93387
 sector 07:  527D6DF6
 sector 08:  00000000
 sector 09:  00000000
 sector 0a:  00000000
 sector 0b:  00000000
 sector 0c:  00000000
 sector 0d:  00000000
 sector 0e:  00000000
 sector 0f:  00000000

 sector 10:  00000000
 sector 11:  00000000
 sector 12:  00000000
 sector 13:  00000000
 sector 14:  00000000
 sector 15:  00000000
 sector 16:  00000000
 sector 17:  00000000
 sector 18:  00000000
 sector 19:  00000000
 sector 1a:  00000000
 sector 1b:  00000000
 sector 1c:  A71B5BA4
 sector 1d:  46FDEA32
 sector 1e:  59621573
 sector 1f:  6B2C8AAD

 sector 20:  309C2800
 sector 21:  32100063
```

## A.2 Hoofddorp


```
readlfx v0.1k (using RFIDIOt v0.1q)
 Reader: ACG LFX 1.0  (serial no: 14070053)
Card ID: UF040C6085C
Tag type: EM 4x02 (Unique) Checking for Q5
   Native - UNIQUE ID: 0f0263103a
```

## A.3 Meppel


```
readlfx v0.1k (using RFIDIOt v0.1r)
  Reader: ACG LFX 1.0  (serial no: 08070045)
Card ID: U80401F0015
Tag type: EM 4x02 (Unique)
  Checking for Q5
    Native - UNIQUE ID: 0102f800a8
```

## A.4 Hoogezand-Sappemeer


```
readlfx v0.1k (using RFIDIOt v0.1r)
  Reader: ACG LFX 1.0  (serial no: 08070045)
Card ID: U80A064458B
Tag type: EM 4x02 (Unique)
  Checking for Q5
    Native - UNIQUE ID: 010526a2d1
```