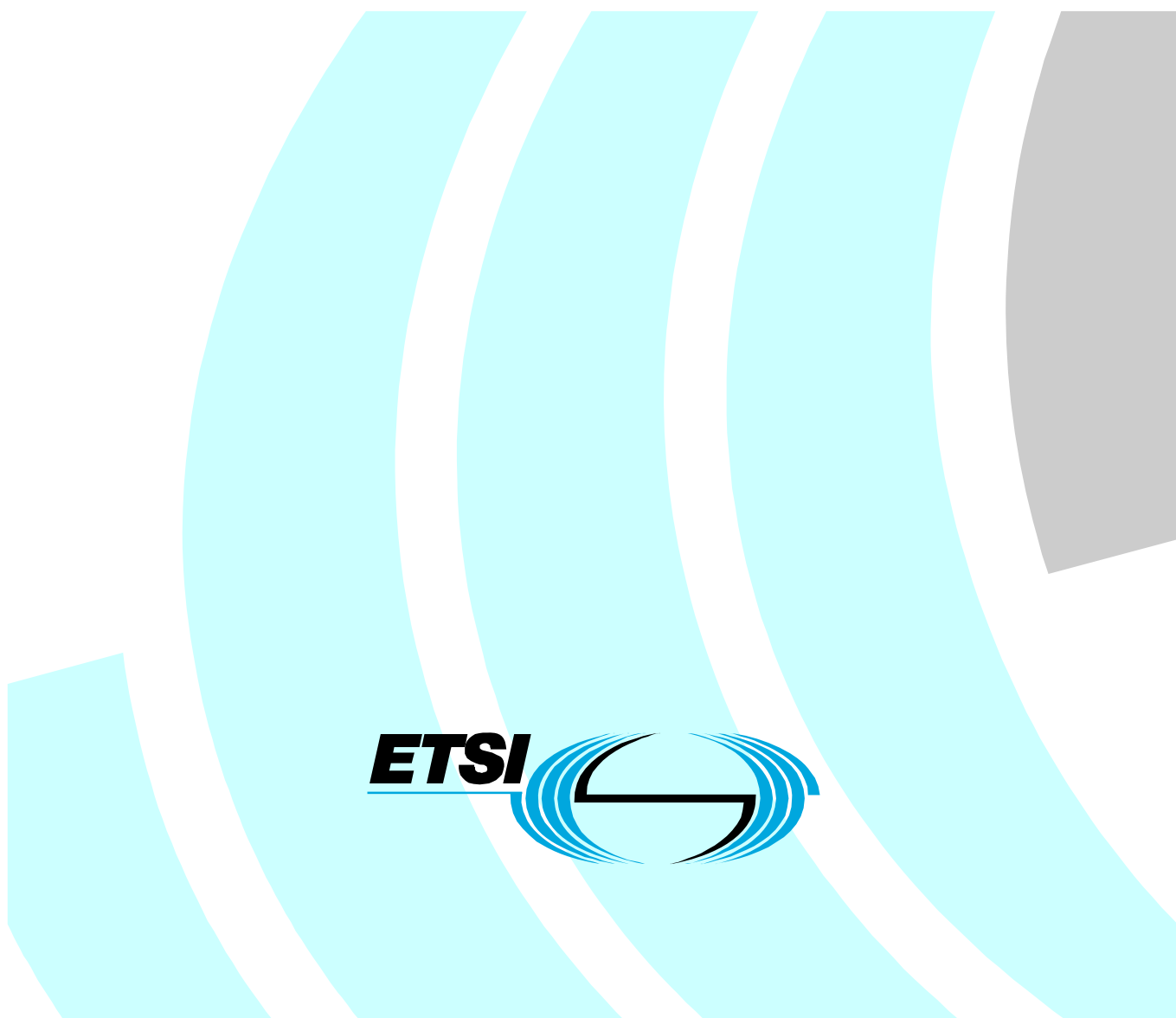


**Electromagnetic compatibility
and Radio spectrum Matters (ERM);
RFID evaluation tests undertaken in support of M/436 Phase 1**



Reference

DTR/ERM-TG34-0100

Keywords

privacy, RFID, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2011.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™**, **TIPHON™**, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

LTE™ is a Trade Mark of ETSI currently being registered

for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	5
Foreword.....	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definitions, symbols and abbreviations	6
3.1 Definitions.....	6
3.2 Symbols.....	7
3.3 Abbreviations	7
4 Introduction	7
4.0 General	7
4.1 Test Area	8
4.2 Equipment	8
4.3 Test Supervisors	9
5 Overview of the Tests.....	9
5.1 Range tests.....	9
5.2 Write Tests	9
5.3 Illicit Reading.....	9
5.4 Eavesdropping.....	10
5.5 Detection inside buildings	10
5.6 Combined EAS/RFID systems	10
5.7 Magnetic fields	10
6 Test procedures and results	10
6.1 Reading range.....	10
6.1.1 Reading range for LF systems	11
6.1.2 Reading range for HF systems.....	11
6.1.3 Reading range for UHF.....	12
6.2 Write range.....	13
6.2.1 Write range at LF.....	13
6.2.2 Write range at HF	13
6.2.3 Write range at UHF.....	14
6.3 Illicit reading	15
6.3.1 Illicit reading of the contents of shopping bags	15
6.3.2 Containers with pills	16
6.3.3 Proximity cards	17
6.3.4 Airline label tag	17
6.3.5 LF tags	17
6.4 Eavesdropping.....	18
6.4.1 LF and HF tests.....	18
6.4.2 Measurements at UHF	18
6.5 Detection inside buildings	18
6.6 Combined EAS/RFID system.....	19
6.7 Magnetic fields	19
7 Visits to operational installations	20
8 Analysis of results	20
9 Conclusions	21
Annex A: Results recorded during the tests	22
A.1 Results of reading tests.....	22

A.2	Results of write tests.....	24
A.3	Noise floor measurements	25
Annex B:	Reports on visits to operational sites.....	26
B.1	Visit to library at Doetinchem	26
B.2	Visit to Metro Future Store	27
Annex C:	Bibliography	29
History	30

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://webapp.etsi.org/IPR/home.asp>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Electromagnetic compatibility and Radio spectrum Matters (ERM).

1 Scope

The present document describes some RFID Evaluation Tests that were carried to evaluate the characteristics and performance of RFID equipment operating at their three principal frequencies of use. The information derived from the tests is directly relevant to the work of STF 396 in preparing their response to EC Mandate M/436 [i.1].

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <http://docbox.etsi.org/Reference>.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] EC Mandate M/436: "Standardisation mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of Information and Communication Technologies Applied to Radio Frequency Identification (RFID) and Systems".
- [i.2] ETSI TR 187 020: "Radio Frequency Identification (RFID); Coordinated ESO response to Phase 1 of EU Mandate M436".
- [i.3] ISO/IEC 14443: "Identification cards -- Contactless integrated circuit cards -- Proximity cards".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

batteryless transponder: transponder that derives all of the power necessary for its operation from the field generated by an interrogator

eavesdropping: illicit reading of the response from a tag that is being activated by an authorised RFID interrogator

effective radiated power: product of the power supplied to the antenna and its gain relative to a half wave dipole in the direction of maximum gain

global scroll: mode in which an interrogator is able to read the same tag continuously for test purposes only

interrogator: equipment that will activate an adjacent tag and read its data

NOTE: It may also enter or modify the information in a tag.

radiated measurements: measurements which involve the absolute measurement of a radiated field

tag: transponder that holds data and responds to an interrogation signal

3.2 Symbols

For the purposes of the present document, the following symbols apply:

A	Amps
dB	decibel
dBm	power level relative to 1 mW
kHz	kilo Hertz
m	metres
MHz	Mega Hertz
mm	millimetres
σ	standard deviation
$\mu\text{A/m}$	micro Amps/metre

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CCTV	Closed Circuit Television
DST	Digital Signal Transponder
e.r.p.	effective radiated power
EAS	Electronic Article Surveillance
HF	High Frequency
IR	Infra Red
LF	Low Frequency
R&TTE	Radio and Telecommunications Terminal Equipment
RFID	Radio Frequency IDentification
SRD	Short Range Device
STF	Special Task Force
UHF	Ultra High Frequency

4 Introduction

4.0 General

The present document describes some RFID Evaluation Tests that were carried out at Nedap on 6th to 8th September 2010. The purpose of the tests was to evaluate the characteristics and performance of RFID equipment operating at their three principal frequencies of use. The information derived from the tests is directly relevant to the work of STF 396 in preparing their response to EC Mandate M/436. Additionally it provided a number of the experts in the STF with the opportunity to witness at first hand the operation of RFID in a number of defined scenarios.

The reason for these tests arose from the apparent lack of any documented work on practical tests that determined the risk of illicitly reading or writing data to tags. The absence of this information has sometimes led to unrealistic claims by the media and other bodies on what is possible. These tests provided information on the capabilities and limitations of RFID when used in a typical operational environment.

The absence of any controlled experiments regarding illicit reading and writing of data is seen by the STF as a major obstacle for consumer acceptance. The uncertainty regarding what is referred to as the actual read and write range and the potential risks has led to confusion and distrust among the public. This particularly includes concerns over the illicit reading and writing to tags. There is also confusion around the various RFID technologies, their capabilities and intended use. The scenarios specified in the tests were intended to address these particular concerns.

4.1 Test Area

The majority of the tests were performed in the meeting area at the Nedap premises. This is a large open plan space with conditions that were considered typical of many environments where RFID might be used operationally. In addition tests were carried out in a mock up of a room in a house, which was also located in the Nedap premises.

The test programme included visits to a working library equipped with RFID and to the Metro Future Store, which uses RFID in its daily operations.

4.2 Equipment

The tests were carried out at the three principal frequencies of use using the equipment listed below:

Low Frequency (< 135 kHz)

- 1) Nedap 120 kHz interrogator XS Accessor III
- 2) DC 1000 Loop antenna
- 3) General purpose LF cards
- 4) TPU Write unit
- 5) TI interrogator RI-TRP-251B-30 and antenna RI-ANT-G01E-30
- 6) Animal tag RI-TRP-0983-30
- 7) Key fob tag RI-TRP-RFOB-30

High Frequency (13,56 MHz)

- 1) Nedap 13,56 MHz Interrogator
- 2) Loop antenna (40 × 150 cm) for library use
- 3) General purpose HF vicinity cards
- 4) Handheld interrogator Quick Scan
- 5) NXP CL RD 701 interrogator driven by Golden Reader Software
- 6) Passport fitted with RFID card
- 7) Transportation card

UHF (865 MHz - 868 MHz)

- 1) Nedap uPASS Reach interrogator
- 2) Nedap Handheld reader
- 3) Prototype interrogator
- 4) Three different designs of retail label tag
- 5) Airline label tag

Test equipment

- 1) Rhode and Schwartz Measurement receiver Type EB200
- 2) Rhode and Schwartz loop antenna Type HFH-Z2
- 3) Rhode and Schwartz spectrum analyser Type ZVL3
- 4) DC Coil for magnetic field DC 190

STF 396 appreciates the assistance given by manufacturers in making their equipment available for these tests. They also wish to thank the staff at the public library at Doetinchem and at the Metro Future Store for hosting conducted visits to their premises.

For the purpose of the tests, RFID tags are defined as batteryless transponders, which only send a response when they are within range of the energising field of an interrogator.

4.3 Test Supervisors

The tests were supervised by the Chairman of ETSI_ERM_TG34 (John Falck) who was assisted by the leader of STF 396 (Scott Cadzow) and Dr. Christian Schenk.

Members of STF 396 who were present at the event were invited to participate in a number of the tests.

5 Overview of the Tests

The tests were divided into six different sections covering each of the main areas of concern. These sections are separately summarised below.

5.1 Range tests

The purpose of these tests was to determine the maximum range at which it was possible to read a tag and to estimate the variability in performance between different tags. Measurements were made at LF, HF and UHF. For the LF and the HF tests, all of the tags had a form factor similar to a credit card. Two variants of the HF tag were supplied, which were the vicinity card and the proximity card. These were tested separately. Three different designs of tag were tested at UHF. They were of different physical sizes and intended predominantly for use as labels in retail applications.

All of the tags tested were batteryless (passive) and were fitted with air cored coils. The tests at UHF included an assessment of the degradation in reading performance of tags when applied to certain materials or affected by the environment or rotated from their optimum orientation.

5.2 Write Tests

These tests measured the maximum distance at which it was possible to write data to a tag. The tests were carried out at all three of the principal operating frequencies. The same tags used in the reading tests were also used for measuring the maximum write range.

5.3 Illicit Reading

These tests covered a range of scenarios that had been raised by the experts during their discussions within the STF. They each represented situations that could arise during the normal course of people's daily lives. They included such situations as monitoring tagged items in shopping bags, as well as plastic bottles/ cartons of pills in handbags. In view of the results showing the limited reading range at LF and HF, it was decided to perform these measurements only at UHF. In addition tests were carried out to assess the ease with which the data in both a passport and a transport card (e.g. Oyster card) could be read. Further measurements were made to determine the range at which it was possible to read an airline tag fitted to a person's suitcase. Finally tests were undertaken to determine the reading range of an animal tag and the ease with which it might be possible to compromise the security of the RFID tag embedded in a key fob.

5.4 Eavesdropping

Concern had been expressed by some members of the STF about the ability of a person with criminal intent to monitor remotely the response from a tag while it was being read by an interrogator. In order to quantify the extent to which this was possible, a tag was continuously activated by an adjacent interrogator. Using a measuring receiver set to high sensitivity, the signal from the tag was repeatedly read at increasing ranges until it could no longer be detected. The results were believed to be indicative of the maximum ranges that eavesdropping would be possible. These measurements were carried out at each of the three main operating frequencies.

5.5 Detection inside buildings

Claims had been made by the press that it was relatively easy for a person to read all of the tags that were inside a person's home. The experts were clearly interested to assess the extent to which this was possible. Tests were performed in a mock-up of a room inside a house. A tagged object was placed at different positions inside the room while an interrogator, which was immediately outside the room, was moved along the 20 cm thick brick wall in an attempt to read the tag. Due to the limited reading range at LF and HF, this test was carried out at UHF only.

5.6 Combined EAS/RFID systems

It had been suggested that a likely spot for an eavesdropper would be at the exit of a shop equipped with a combined EAS/RFID system. The experts wished to know whether the handheld reader might adversely affect the performance of the EAS/RFID equipment located at the exit as shoppers left the premises. Similarly there was also a concern that the EAS/RFID equipment would influence the performance of a handheld reader being used to read tags illicitly. Tests were therefore carried out to determine if either of these effects was evident.

5.7 Magnetic fields

TR 187 020 [i.2], which had been circulated for Public Enquiry, included a statement saying that RFID tags were susceptible to damage from magnetic fields. There was no independent reference in the document to support this statement so it was decided to carry out a test to investigate if it was correct. A LF tag was placed in close proximity to a calibrated coil. The maximum range at which the tag could be measured both with and without a current passing through the coil was compared. Since LF is the closest frequency to d.c. it was considered unnecessary to repeat this test at HF and UHF.

6 Test procedures and results

Both before and after the tests, measurements were made of the noise floor levels at each of the three frequencies of interest. The results are shown on table A.5.

These levels were considered typical of what might be experienced in the environments where RFID systems would be deployed.

A description of the procedure for carrying out each of the tests together with details of the test results is provided below.

6.1 Reading range

Tests on the reading range at each of the three principal operating frequencies were performed in accordance with the Test Plan. Details on each of the tests are provided below.

6.1.1 Reading range for LF systems

A loop antenna of approximate dimensions 40×80 cm was positioned so that its centre was level and parallel with a wooden table. The loop antenna was connected to a Nedap 120 kHz interrogator. The field generated by the loop when powered by the interrogator was measured and found to be $59 \mu\text{A}/\text{m}$ @ 10 m. A ruler was laid along the length of the table. With the loop antenna energised by the interrogator, a tag in its optimum orientation with respect to the loop was moved slowly towards the antenna. See figure 1.



Figure 1: Measuring reading range at LF

The distance at which the tag was first read by the interrogator was recorded. The tag was moved slowly away from the loop until it just ceased to be read and the distance was again recorded. This procedure was repeated three times.

The same process was repeated for a further nine tags. The results from the measurements are shown in table A.1.

It will be seen from the results that the average range of an LF tag under the test conditions described above is 88 cm. Also there was only a difference in reading range of about 2 cm when moving the tag towards the loop and moving it further away. Based on a very small sample size, the vast majority of LF tags would have reading ranges of between 82 cm and 93 cm.

6.1.2 Reading range for HF systems

These tests used a loop antenna configured in the form of a figure of eight as supplied by Nedap for their library system. The centre of the lower loop was arranged to be level with a wooden table. The loop was connected to an interrogator operating at 13,56 MHz. The field generated by the loop antenna was $53,5 \text{ dB}\mu\text{A}/\text{m}$ @ 10 m.

With the interrogator set to transmit continuously, a vicinity tag in its optimum orientation was moved slowly towards the loop antenna. See figure 2.



Figure 2: Measuring reading range at HF

The distance at which the vicinity tag was first read by the interrogator was recorded. The tag was moved slowly away from the loop antenna until it just ceased to be read and the distance was again recorded. This test was repeated three times.

The same process was repeated for a further twenty four vicinity tags. The results from the measurements are shown in table A.2.

The average range of an HF vicinity tag under the test conditions described above was 82 cm. Also there was only a difference in reading range of about 2 cm when moving the vicinity tag towards the loop and moving it further away. Although the sample size was small, a large population of HF vicinity tags could be expected to have reading ranges of between 85 cm and 78 cm.

6.1.3 Reading range for UHF

These tests were performed using the Nedap uPASS Reach interrogator, which combined the functions of antenna and interrogator within a single case. The unit was arranged to be at the same height as a wooden measuring table as shown in figure 3.



Figure 3: Measuring reading range at UHF

The conducted power from the interrogator was measured at 27,7 dBm, which was equivalent to a radiated power of 33,25 dBm e.r.p. The equipment operated in the band 865 MHz to 868 MHz.

The tests on reading range were performed on three different designs of retail tag. With the interrogator switched on, a tag in its optimum orientation with respect to the transmission was moved slowly towards the coil. The distance at which the tag was first read by the interrogator was recorded. The tag was moved slowly away from the interrogator until it just ceased to be read and the distance was again recorded. This procedure was repeated three times.

The same process was performed for a further ninety nine tags. The results from the measurements are shown in table A.3.

The average range of an UHF tag under the test conditions described above was 345 cm. Also typically there was only a difference in reading range of about 3 cm when moving the tag towards the loop and moving it further away. Although the sample size was small, large populations of UHF tags could be expected to have reading ranges of between 372 cm and 315 cm.

During the course of the tests at UHF, it was demonstrated that the reading range was affected by a number of factors. For instance the nature of the material to which the tag was attached could modify the performance. This was particularly apparent for objects containing either water or metal. Mis-orientation of the tag from its optimum alignment and changes to the environment also reduced the reading range. For example it was shown that the movement of people in the immediate vicinity of the interrogation zone could have a noticeable effect. It was also demonstrated that shielding of the tag by means of aluminium foil prevented the tag from being read.

6.2 Write range

Tests to measure the distance at which it was possible to write to a tag were carried out at LF, HF and UHF. A description of each of these tests is provided below.

6.2.1 Write range at LF

These tests were performed using a purpose made writing unit. A picture of the equipment is shown in figure 4.



Figure 4: Measuring write range at LF

Tests on the maximum range at which it was possible to write data were carried out on five tags. The tags were progressively moved further away from the antenna until writing was no longer possible. The range at which this occurred for each tag is summarised in table A.4.

The typical maximum write range was 4,6 cm with no tag functioning above 6 cm.

6.2.2 Write range at HF

At HF it was possible to write to a vicinity card using the same equipment set up as used for the reading tests. The maximum range at which it was possible to write data was measured for five vicinity cards. The results are shown in table A.4.

Typically the write range for a HF vicinity card was 60 cm with the vast majority of cards having a write range of less than 80 cm.

6.2.3 Write range at UHF

Measurements of the write range at UHF were performed on a prototype interrogator. See figure 5.

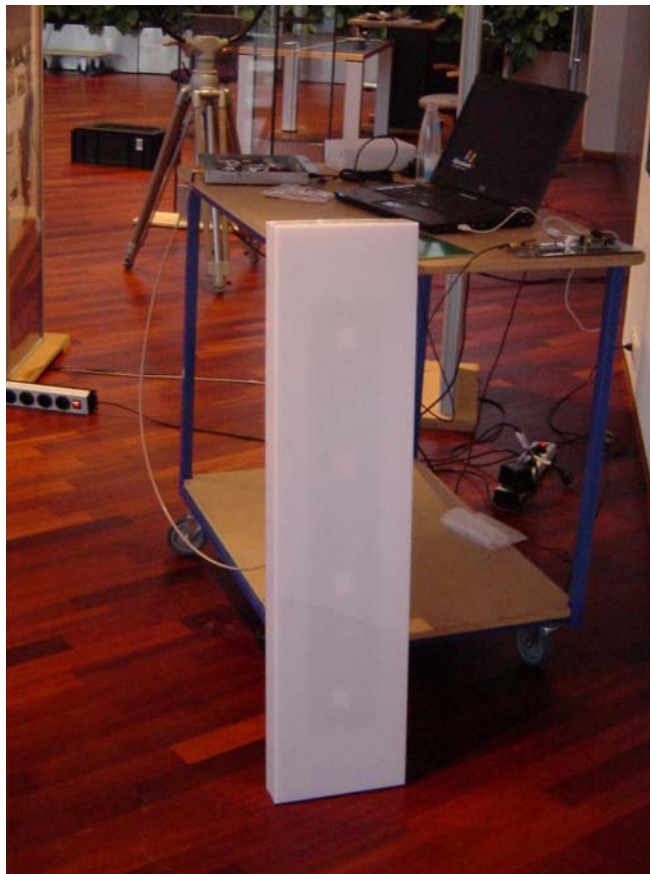


Figure 5: Write range equipment at UHF

Conducted measurements on the prototype interrogator showed that it was set to a level of 28,1 dBm, which was equivalent to a transmitted power level of 34,6 dBm e.r.p. This exceeded the permitted limit by 1,6 dB.

Measurements were made on a sample of five UHF retail tags taken from the same batch that had been used in the tests for reading range. It was immediately apparent that the reading range was considerably greater than what had been recorded previously. Measurements were therefore made for both the reading and write ranges. These are summarised in table A.4.

From the results it can be seen that the average reading range had increased to 8,6 m with one tag achieving a figure of 9,75 m. In all cases the maximum write range was approximately 1 m less than the read range.

Subsequently an investigation was made into the differences in reading range between the two types of interrogator. The Nedap design engineer said that the receiver in the uPASS Reach interrogator had been designed with a sensitivity of typically -62 dBm. This level had been selected because it met the needs of the intended applications. The prototype interrogator had a sensitivity that was estimated to be at least 10 dB greater.

It was also explained that the retail tags used in the tests contained the latest design of integrated circuits manufactured by Impinj. The sensitivity of these integrated circuits has been improved allowing them to operate at approximately 2,5 times the range of the first generation devices. However, because of the improved sensitivity the signal received at the interrogator has to be increased to hear the tags at maximum range.

From theory if the power level of the prototype interrogator was reduced from 34,6 dBm to its maximum permitted limit of 33 dBm e.r.p, its reading range in free space would be reduced by 17 %. Using the average figure for range of 8,6 m in table A.4, this would equate to an adjusted average range of 7,2 m at 33 dBm e.r.p.

Nedap provided a sample of a tag that was intended for use with their uPASS Reach interrogator. When tested in its optimum orientation in free space it was just possible to achieve a read range of 7,0 m. This showed that, during the tests in clause 6.1.3, the uPASS Reach interrogator had been receive range limited and explained the reduced reading performance.

6.3 Illicit reading

These tests comprised a set of scenarios covering concerns that have been raised over the threats posed by RFID to privacy and security. A description of the method of test and the results for each scenario is provided below.

6.3.1 Illicit reading of the contents of shopping bags

All of the tests were carried out at UHF. Three shopping bags, coloured orange, white and blue respectively, were each filled with five identical tagged items. In order to optimise the conditions for most favourable reading, none of the tagged items contained any water or metal. See figure 6. The identity number of each of the tags was recorded.



Figure 6: Contents of tagged items in shopping bag

A handheld reader (figure 7) was used to simulate the illicit reading of the contents of the shopping bags.



Figure 7: Hand held reader

In the initial tests reading was attempted first with a stationary person carrying a shopping bag and then with the same person walking across the room. In both cases it was necessary to bring the handheld reader within 60 cm of the shopping bag before the contents of the bag could be read. During this test the lady carrying the bag commented that the reading process had represented an intrusion into her personal space.

The test was modified so that the shopping bags were carried by three people walking side by side. The first person carried a bag in the left hand, the centre person in the right hand and the third person in the left hand. Thus two of the bags were immediately adjacent to each other. In order to read the tagged items, the hand held reader was passed immediately behind the bags at a distance of about 60 cm. The results are shown in table 1.

Table 1: Analysis of illicit reading of shopping bags

Serial No	Tag number	Colour of bag
1	AD99210442528F9260000DF	O
2	AD99210442527D8F5F0000DC	B
3	AD992104425249915D0000D7	B
4	AD992104425249925E0000D6	B
5	AD9921044252918F610000DE	B
6	AD9921044251E590630000CA	W
7	3005FB63AC1F3841EC880467	B
8	AD9921044252A990620000E2	O
9	AD9921044252758E5F0000DB	W
10	AD99210442527B9260000DD	O
11	AD9921044251E391630000CB	W
12	AD99210442529790610000E0	O
13	AD9921044252618C5D0000DA	W
14	AD992104425259935E0000D9	W
Key: B = blue W = white O = orange		

From the table it can be seen that only 14 out of the fifteen tags were read. Perhaps of greater interest is that the order in which the tags were read was apparently random. Thus it would not be possible from the results to say with any certainty which items were in each of the bags.

6.3.2 Containers with pills

In a second scenario UHF tags were attached to two plastic bottles and to a carton, all of which contained pills. The pills in the carton were encapsulated in packing with a silver foil backing. See figure 8.

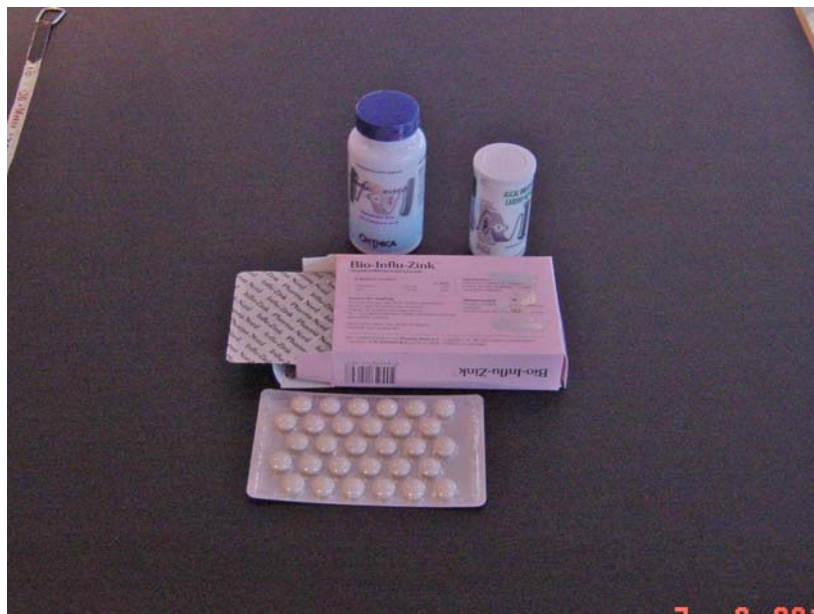


Figure 8: Tagged bottles and box of pills

A bottle was placed in each of two ladies handbags. Using the hand held reader the tags could be read inside the handbags at distances between 65 cm and 90 cm.

The reading range of the carton of pills was measured with the tag facing the reader (i.e. the silver foil furthest from the reader). In this setup the tag could be read in free space at a distance of 23 cm. With the carton placed in a lady's handbag and the silver foil facing the reader, it was not possible to read the tag. However when the carton was rotated so the tag was no longer shielded by the silver foil, the achievable reading range increased to between 80 cm and 120 cm. The reason for this increase was not immediately clear and was attributed to the undisclosed contents inside a lady's handbag!

6.3.3 Proximity cards

A further scenario included reading both the proximity tag in passports and in RFID transportation cards (such as the Oyster card). Both types of tag operate at HF using the ISO/IEC 14443 [i.3] technology. Reading the tags was performed using the NXP CL RD 701 (general purpose) interrogator. In all cases the reading range was less than 10 cm. It was explained that both tags incorporated security features, which protected them from being interrogated by normal commercially available equipment. In the case of the passport it was not possible to recover the data in the tag without first transmitting an algorithm based on the machine readable code printed on the page containing the personal details of the holder. For the transportation card it was necessary for the interrogator to initiate an encrypted dialogue with the tag. This was believed to provide sufficient security to prevent illicit reading by a non-professional criminal.

6.3.4 Airline label tag

A separate measurement was made of the reading range of an airline label tag that is used to route and identify a passenger's baggage. The measurement was carried out using the uPASS Reach interrogator, which gave a reading range of approximately 4 m. If the measurement had been repeated using the prototype interrogator it is very possible that the reading range would have been in excess of 10 m.

6.3.5 LF tags

Finally two LF tags were measured using an interrogator provided by Texas Instruments. One of the tags was intended for the identification of farm animals and was approximately 30 mm in length. Normally it would be used either in a plastic eartag, or put into a ceramic housing for use as a ruminal bolus transponder for cattle or sheep or inserted under the skin. The second tag was designed for use in the key fob of a car as a security measure. The coils in both tags were wound on ferrite cores.

The tags were read using a loop antenna that was approximately 70 cm × 40 cm in size. This was significantly larger than would normally be used for the above two applications.

With the tags held in optimum orientation approximate reading ranges of 30 cm and 15 cm were recorded for the animal tag and key fob tag respectively. Subsequently it was discovered that another LF interrogator was operating in an adjacent room. When this was switched off, the range of the animal tag increased to 50 cm. This demonstrated very effectively the susceptibility of RFID systems to ambient noise. Frequently the maximum ranges quoted by manufacturers are significantly greater than the distances that can be used for reliable operation.

It was explained that the animal tag contains only a fixed number. This same number is also held in a central database. Identification of the animal can only be achieved by access to the database. However simply knowing the number would be sufficient to enable movements of the animal to be tracked.

Since the key fob tag is intended as an anti-theft device it incorporated a number of security features. In normal use the tag operates at very close range so monitoring its response from outside the car would be technically difficult. In addition the system uses an authentication technique known as DST (Digital Signature Transponder) and includes a rolling code. It was comforting to note that although the interrogator was able to read the demonstration tag, it was unable to read the tag in a key fob owned by one of the supervisors.

6.4 Eavesdropping

These tests were designed to measure the distance at which it would be possible to detect the response from a tag that was being activated by another RFID system. The tag responses were measured using conventional high quality laboratory equipment, which were able only to indicate that a tag signal was present. In order to decode the signal it would have been necessary to develop special purpose-built receivers. It should be noted that the distance at which it is possible to read a tag is always less than the distance at which it is possible to detect its presence. The measurements were performed at LF, HF and UHF.

6.4.1 LF and HF tests

The measurement method for monitoring the tag responses at LF and HF was the same. A Rhode and Schwartz loop antenna was connected to a Rhode and Schwartz measuring receiver. The interrogator was set-up to activate an adjacent tag continuously. The response from the tag was most effectively detected as an audible signal at the measuring receiver. The maximum distances at which it was possible to detect the various types of tags are summarised below.

Table 2: Maximum distances for eavesdropping with LF and HF tags

Type of Tag	Distance - metres
LF systems	
Standard card for LF use	2,6
HF systems	
Vicinity cards	3,5
Passport	2,6
Oyster cards	3,0

6.4.2 Measurements at UHF

Measurements at UHF were made using a log-periodic antenna connected to a spectrum analyser. The response from the tag was best viewed as a data stream on the display. Since the responses from the tags at UHF were true radio waves, they could be detected at much greater distances than were possible at HF and LF. With the uPASS Reach interrogator set-up to activate continuously an adjacent retail tag, the measuring antenna was orientated to receive maximum signal. The distance between the tag and the measuring antenna was then progressively increased until it was no longer possible to see the data stream on the spectrum analyser.

It was demonstrated that it was possible to detect the response from the tag at distances up to 100 m across an open space immediately outside the Nedap building.

6.5 Detection inside buildings

The tests were carried out in a mock-up of a room inside a house using first the uPASS Reach interrogator and then the hand held reader. A retail tag was attached to a box of chocolates.

The interrogator was positioned at a distance of approximately 15 cm from the outside wall of the room. The interrogator was directed at the wall and switched on in continuous read mode. With the tag on the box of chocolates nearest the interrogator and in optimum orientation, it was held at a distance of about 20 cm from the wall and moved until it was read. It was then moved slowly away from the wall until detection was lost. This occurred at a distance of about 1 m.

The box of chocolates was then moved back to a distance of 20 cm from the wall and moved laterally until reading ceased. This took place for movements of approximately half a metre on either side of the optimum reading position.

An attempt was made to read the tag through the wall using the hand held reader. This proved not to be possible. However the tag could be read by the hand held reader through the glass of the door to the room at a distance of about 5 cm.

6.6 Combined EAS/RFID system

A typical EAS/RFID system operating at UHF, such as might be seen at the exit from a shop, was set up in the meeting area. The system was switched on and a shopping bag containing five tagged items was carried through the gate to verify that it raised an alarm.

A hand-held reader also operating at UHF was held close to the exit of the gate and activated. The shopping bag with the tagged items was again carried through the gate. There was no apparent detrimental effect on detection of the tagged items for both the gate system and the hand held reader. The test was repeated with the hand-held reader held on the "approach side" of the gate with the same result.

6.7 Magnetic fields

The test was performed at LF only using a calibrated coil of 171 mm × 147 mm consisting of 40 turns. When a current of 5 A was passed through the coil it generated a magnetic field of 1,432 A/m. The test was carried out with one of the air cored passive tags that had been used in the previous tests.

For the tests the system was configured so that the tag was separated by a distance of approximately 2 cm from the surface of the coil. See figure 9.



Figure 9: Set-up for magnetic field test

The tag was placed in optimum orientation with respect to the loop antenna. With no current passing through the coil, the tag was moved to a position where it could only just be read by the interrogator. Without moving the tag a current of 5 A was passed through the coil. It was noted that the presence of the magnetic field had no effect on the reading range.

7 Visits to operational installations

The test programme included visits to two operational sites that were equipped with working RFID systems. These were at the public library at Doetinchem and to the Metro Future store. Reports on these visits are provided in annex B.

8 Analysis of results

It was recognised from the outset that the test environment was assumed to be typical of what might be found in operational installations and that the results were therefore no more than indicative of what might be experienced in practice.

The results for reading and writing ranges showed that the performance of tags in free space is remarkably consistent. However there is a considerable difference in the performance of inductive systems (LF and HF) and those operating at UHF. Although the reading range of tags at UHF is greater, they are affected more by the items to which they are attached and by their orientation. Also reading performance is more sensitive to the immediate environment. For example transmissions are easily reflected or shielded and are modified by the presence of people/objects moving in the immediate area of the interrogation zone. All systems are influenced by the presence of ambient noise.

Due to the influences described above, for acceptable performance RFID systems are usually designed to operate well within the maximum limits specified by the manufacturers. Typically the maximum usable ranges for most LF and HF proximity systems are less than 60 cm. For vicinity systems operational ranges are of the order of 2 cm to 5 cm. For systems at UHF reading ranges up to 5 m are realistically possible, although very often systems are designed with ranges of about 3 m.

In very many applications the data in the tag remains unchanged for much of its life. Modification of the data on a regular basis is confined largely to industrial installations and to high security applications such as financial transactions. In the latter case the operational ranges are of the order of 2 cm to 5 cm.

Illicit reading with a portable reader is possible at ranges of up to 60 cm. This is sufficiently close to be uncomfortable for the intended victim. Reading tags carried by a single person in an open space may therefore arouse suspicion. On the other hand in situations where a number of people, all carrying tagged items, are in close proximity with each other, it would be very difficult to determine which tags are being carried by each person.

Alternatively illicit reading may be performed using a fixed long range interrogator. For this to be effective the interrogator would have to be coupled to a second device such as a CCTV camera. Also unless the activity was carried out in a quiet area, it would be difficult to identify which individuals were carrying tags.

Greater reading ranges (up to 1,2 m) using a hand held reader were possible for tagged cartons of pills in ladies handbags, although this was dependent on the way in which the cartons were positioned. The reason for this is not understood and might represent an area for further study.

The very short operational ranges of vicinity cards and key fob tags make them unlikely targets for illicit reading. Additionally they are further protected by means of authentication and encryption techniques. However they may be a target for professional criminals who might develop alternative means of attack.

Technically eavesdropping would be possible at all three frequencies. However the limited distances at which this could be achieved at LF and HF makes this less likely. On the other hand, given a clear propagation path, it would certainly be possible covertly to read the contents of UHF tags at significant distances. However the value gained from this activity is questionable. Without multiple receivers located at different locations, it would be very difficult to determine the position of the tag that had been read. This would necessitate a clear propagation path to the tag for each receiver. The situation would be further complicated if there were multiple RFID installations in the same area. This could mean that tags from the different installations could respond simultaneously. Unless there were substantial differences in the signal strengths received from the different tags, it would be impossible to decode them and determine their positions. It is important therefore to evaluate carefully both the value to the attacker and the extent of the risk posed by eavesdropping.

Based on the results the probability of reading tagged items inside a house from outside is likely to be low. The tagged items would need to be close to an outside wall and in optimum orientation with respect to the antenna held by the attacker. Also given the attenuation of the signal through the wall, the attacker would need previous knowledge of the positions of tags in order to read them. Many criminals might well consider that the difficulties involved did not justify the effort.

It should be remembered that some of the tests inside a house were carried out using the uPASS Reach interrogator and a tag containing an Impinj chip. As was discovered during the writing tests, this was not the preferred combination. It may be prudent to repeat the tests with another RFID system.

The tests on the EAS/RFID system showed that it was unaffected by the immediate presence of a handheld reader.

The tests showed that a strong magnetic field had no detrimental effect on reading performance. This test was carried out using an LF tag that was constructed with an air core. It might be instructive to repeat this test using a tag with a ferrite core.

9 Conclusions

Based on the results and the subsequent analysis, the following conclusions may be drawn from the tests.

The tests covered a wide range of scenarios and generated a lot of valuable information for use by the STF.

The tests demonstrated that there is a clear difference in the characteristics of inductive RFID systems (LF and HF) and systems that operate at UHF. These differences should be taken into account during the work of the STF.

The risks attributed to illicit reading are probably less than had previously been thought.

The responses from tags operating at UHF can be read at significant distances. The STF should assess very carefully the extent of the risks that this creates for the privacy and security of the public.

The tests could find no evidence that a high magnetic field can cause damage to RFID tags.

The results from the present document could be used to identify areas for more detailed investigation in future tests.

Annex A: Results recorded during the tests

A.1 Results of reading tests

Table A.1: Reading range results for LF tags

Serial No.	1st measurement		2nd Measurement		3rd Measurement		Mean range	
	In (cm)	Out (cm)	In (cm)	Out (cm)	(cm)	Out (cm)	In (cm)	Out (cm)
100	83	90	83	92	85	88	83,67	90,00
99	87	91	88	89	86	89,5	87,00	89,83
97	88,5	88,8	86,5	87	85	87	86,67	87,60
96	87	87,5	85	88	85	86	85,67	87,17
95	88	89	87	88	89	89	88,00	88,67
94	90	91	90	91	91	92	90,33	91,33
93	87,5	89	88,5	91	91	91,5	89,00	90,50
92	86	89	86	89,5	87	90	86,33	89,50
91	88	91	87	91	87	88	87,33	90,00
90	87	90	89,5	91	86,5	88	87,67	89,67
Arithmetic mean							87,17	89,43
Standard deviation σ							1,82	1,28
Two standard deviations 2σ							3,64	2,56
Max read range of approx 95% of tags will fall between						Upper	90,81	91,98
						Lower	83,53	86,87

Table A.2: Reading range results for HF tags

Serial No.	1st measurement		2nd Measurement		3rd Measurement		Mean range	
	In (cm)	In (cm)	In (cm)	In (cm)	In (cm)	In (cm)	In (cm)	In (cm)
1	80	80	79,5	79,5	79,3	82,5	79,60	80,67
2	80,3	80,5	80,2	78	80,5	79	80,33	79,17
3	80,6	81,9	80,7	81	81	82	80,77	81,63
4	80,8	82,5	80,8	80	80,7	80	80,77	80,83
5	79,4	81,7	79,6	84	79,7	86	79,57	83,90
6	79,8	81,6	80,1	87	80,3	88	80,07	85,53
7	78	80,6	78,5	78	78,6	77	78,37	78,53
8	80,1	81,2	80,2	84	80,6	83	80,30	82,73
9	81	81,6	81,5	79	81,6	78	81,37	79,53
10	81,3	81,5	80,8	86	81,6	86	81,23	84,50
11	80,6	83	81	82	81,1	84	80,90	83,00
12	80,7	81	81	85	81,4	84	81,03	83,33
13	79,9	78,3	80	80	80,1	80	80,00	79,43
14	79	78,1	79,1	83	79,1	85	79,07	82,03
15	79,9	81	79,5	81	79,3	82	79,57	81,33
16	80	80,2	80,3	85	80,5	86	80,27	83,73
17	79	79	79,5	81	79,3	81	79,27	80,33
18	78,9	82	79,4	81	79,6	82	79,30	81,67
19	79,3	81,8	79,6	84	80,4	84	79,77	83,27
20	80,5	81	80,9	84	81	85	80,80	83,33
21	79,5	80,6	79,9	81	80	83	79,80	81,53
22	81	80,5	80,6	79	80	79	80,53	79,50
23	81	82	81,2	80	81,8	83	81,33	81,67
24	81,4	80,5	81,5	83	81	81	81,30	81,50
25	80	81,5	81	79	80,8	79	80,60	79,83
Arithmetic mean							80,24	81,70
Standard deviation σ							0,80	1,83
Two standard deviations 2σ							1,60	3,67
Max read range of approx 95% of tags will fall between						Upper	81,83	85,37
						Lower	78,64	78,03

Table A.3: Reading range results for UHF tags

Batch 1	Serial No.	1st measurement		2nd measurement		3rd Measurement		Mean range (cm)	
		In (cm)	In (cm)	In (cm)	In (cm)	In (cm)	In (cm)	In (cm)	In (cm)
	1	3,43	3,48	3,44	3,47	3,46	3,48	3,44	3,48
	2	3,22	3,27	3,24	3,27	3,24	3,26	3,23	3,27
	3	3,4	3,43	3,41	3,43	3,41	3,42	3,41	3,43
	4	3,46	3,49	3,47	3,49	3,47	3,49	3,47	3,49
	5	3,44	3,49	3,47	3,49	3,47	3,49	3,46	3,49
	6	3,46	3,5	3,46	3,49	3,45	3,49	3,46	3,49
	7	3,41	3,47	3,42	3,46	3,43	3,48	3,42	3,47
	8	3,45	3,49	3,46	3,49	3,47	3,49	3,46	3,49
	9	3,48	3,52	3,48	3,52	3,48	3,51	3,48	3,52
	10	3,42	3,46	3,42	3,45	3,42	3,43	3,42	3,45
	11	3,44	3,49	3,43	3,48	3,45	3,48	3,44	3,48
	12	3,46	3,51	3,47	3,51	3,47	3,5	3,47	3,51
	13	3,42	3,5	3,45	3,5	3,46	3,51	3,44	3,50
	14	3,43	3,5	3,45	3,5	3,46	3,5	3,45	3,50
	15	3,45	3,51	3,46	3,5	3,45	3,49	3,45	3,50
	16	3,43	3,49	3,48	3,49	3,45	3,51	3,45	3,50
	17	3,44	3,51	3,45	3,52	3,47	3,52	3,45	3,52
	18	3,39	3,49	3,45	3,5	3,46	3,52	3,43	3,50
	19	3,44	3,49	3,45	3,49	3,46	3,5	3,45	3,49
	20	3,23	3,28	3,24	3,27	3,3	3,34	3,26	3,30
	21	3,47	3,53	3,47	3,52	3,47	3,5	3,47	3,52
	22	2,7	2,8	2,77	2,8	2,77	2,8	2,75	2,80
	23	3,47	3,51	3,47	3,5	3,47	3,5	3,47	3,50
	24	3,39	3,43	3,23	3,27	3,17	3,18	3,26	3,29
	25	3,45	3,49	3,47	3,5	3,47	3,5	3,46	3,50
Batch 2	1	3,47	3,5	3,48	3,51	3,48	3,5	3,48	3,50
	2	3,46	3,49	3,47	3,49	3,47	3,49	3,47	3,49
	3	3,6	3,62	3,6	3,62	3,61	3,63	3,60	3,62
	4	3,48	3,5	3,48	3,5	3,48	3,5	3,48	3,50
	5	3,47	3,5	3,47	3,5	3,48	3,5	3,47	3,50
Batch 3	1	3,44	3,48	3,45	3,48	3,44	3,47	3,44	3,48
	2	3,45	3,48	3,42	3,46	3,44	3,47	3,44	3,47
	3	3,48	3,49	3,48	3,48	3,48	3,49	3,48	3,49
	4	3,41	3,43	3,41	3,43	3,41	3,42	3,41	3,43
	5	3,43	3,47	3,43	3,46	3,45	3,48	3,44	3,47
				Arithmetic mean				3,42	3,45
				Standard deviation σ				0,13	0,13
				Two standard deviations 2σ				0,27	0,26
				Max read range of approx 95% of tags will fall between		Upper		3,69	3,72
						Lower		3,15	3,19

A.2 Results of write tests

Table A.4: Results of write tests

LF Tests

Serial No.	Tag Type	Point where write fails (cm)
1	Card	3.5
2	Card	4.5
3	Card	4.5
4	Card	6
5	Card	4.5

Arithmetic mean	4.6
Standard Deviation σ	0.89
Two standard deviations 2σ	1.79
Max write range of 95% of tags will fall between	6.39
	2.81

HF Tests

Serial No.	Tag Type	Point where write fails (cm)
26	Proximity	64
27	Proximity	54
28	Proximity	71
29	Proximity	61
30	Proximity	46

Arithmetic mean	59.2
Standard Deviation σ	9.58
Two standard deviations 2σ	19.15
Max write range of 95% of tags will fall between	78.35
	40.05

UHF Tests

Serial No.	Max read range (m)	Point where write fails (m)
1	7.85	7.05
2	8.2	6.9
3	8.5	7.4
4	8.9	8.04
5	9.75	9

Arithmetic mean	8.64	7.678
Standard Deviation σ	0.73	0.86
Two standard deviations 2σ	1.46	1.72
Max write range of 95% of tags will fall between	10.10	9.40
	7.18	5.96

A.3 Noise floor measurements

Table A.5: Noise floor measurements

Frequency range System	Measuring Frequency Range	Measuring Bandwidth	System Bandwidth	Noise Measurements in dBµV/m Unless otherwise noted			Type of noise and source	Source
				1	2	3		
		kHz	kHz					
LF-Nedap	116-119,5 kHz	0,150	2	41	43	41	Broadband	External
	120,0 kHz	0,150		98	82	85	Unmodulated Carrier	Neighbouring Nedap systems
	120,5-124 kHz	0,150	2	41	41	54	Broadband	External
LF-Texas Instruments	124-138 kHz	0,150	2	46	51	61	Broadband	External
	129 kHz	0,150		60		58	Radio Signal	External
	135 kHz	9			48		Radio Signal	External
HF Mifare	12,64-12,79 MHz	9	150	<36*	42	40	Broadband	External
	12,64-12,71 MHz	9			45		Small band RFI	Battery Charge
	14,33-14,48 MHz	9	150	<36*	<36*	<36*	Broadband	External
	14,36-14,43 MHz	9			42		Small band RFI	Battery Charge
HF-Vicinity	12,72 MHz	9			32		Radio Signal	External
	13,11-13,16 MHz	9	50	<31,5*	34,5	35,5	Broadband	External
	13,17 MHz	9			47		Small band RFI	Battery Charge
	13,95-14,01 MHz	9	50	<31,5*	<31,5*	35,5	Broadband	External
UHF	13,96 MHz	9			35		Small band RFI	Battery Charge
	865-868 MHz	150	150	<26,5=<-104 dBm	-	<26,5=<-104 dBm	Broadband	Noise floor measurement receiver
	865,7;866,3;866,9;867,5 MHz	150	150	-95 dBm	-	-95 dBm	Small band carrier +modulation	Neighbouring Nedap systems
*If < is indicated, then the measured level is the noise floor of the measurement receiver								
*The system bandwidth is indicating where the measured noise is broadband, and the field strength is recalculated from the noise power in the receiver bandwidth to the total noise power in the system bandwidth								
Noise measurement 1 is performed on Monday 6 th , 2010 before the start of the tests								
Noise measurement 2 is performed on Monday 6 th , 2010 after the tests								
Noise measurement 3 is performed on Tuesday 7 th 2010 before the start of the test								

Annex B: Reports on visits to operational sites

B.1 Visit to library at Doetinchem

The public library at Doetinchem holds approximately seventy thousand books and a further number of DVDs. All of these items have been fitted with RFID tags operating at 13,56 MHz. The tags have a similar form factor to a credit card and are attached to the inside cover of each book. The data in the tag comprises the following information:

- The identification number of the card.
- The identification number of the book.
- Details concerning any associated annexes.
- An identifier denoting the name of the library.

All of this information is stored in a central data base within the library.

In normal operation authorised customers may take out books on loan and return them without intervention by the library staff. To take out a book it is only necessary to place the selected book on a reading point at the checkout station. See figure B.1.



Figure B.1: Library checkout table

Having read the tag in the book, the customer is then invited to enter some personal details. This information is logged in the central data base and the customer is authorised to take the book out on loan.

The reverse process takes place for the return of the book. However for this activity the central database checks that the book has been returned within the authorised loan period. If the book is overdue, the customer is required to pay a fee. Once the book has been checked in, the customer posts it through a slot into a "returned books" container.

An EAS/RFID gate is installed at the exit to the library. See figure B.2.



Figure B.2: EAS/RFID reader at library exit

This will alarm in the event that anybody attempts to steal a book or remove one without having correctly completed the check-out procedure.

The management of the library were very pleased with the operation of the system and claimed that it had significantly improved their efficiency.

B.2 Visit to Metro Future Store

The Metro Future Store is used by Metro to test new and innovative marketing concepts. In addition to experimenting with an impressive range of new ideas, it also includes two applications for RFID. The first of these was located at the goods receiving area and the second was used to control the operation of the fresh meat counter. The experts from the STF were shown both installations.

In the goods receiving area RFID had been installed at both dock doors and at the interface between the back of store and front of store. Portals containing four antennas were mounted at each reading point. See figure B.3.



Figure B.3: RFID Portal at goods receiving at Metro

The antennas were driven by an interrogator that energised each one in turn according to a pre-defined switching sequence. The interrogator was connected to the store's computer system. Operation of each interrogator was triggered by an IR curtain, which was positioned above the portal.

The system was used to read tags that were attached to pallets and cartons as they passed through each portal. The system provided greater reliability than manual operation and was less labour intensive.

The second application at the fresh meat counter is used to control the transfer of fresh meat. See figure B.4.



Figure B.4: Fresh meat counter at Metro

Each portion of meat is placed on a polystyrene tray and covered with cellophane. A tag is attached to each tray. An array of antennas is mounted below the meat counter. This allows the meat trays at the counter to be read repeatedly at regular intervals. This means that stocks of meat on display can be kept to an economic minimum and be replenished only when necessary. With the present legislation on the handling of fresh meat, the RFID system ensures compliance with the legal requirements and simplifies the materials handling process.

Annex C: Bibliography

Terms of Reference for Specialist Task Force STF 396 (CEN/CENELEC/ETSI) "Response to Phase 1 of EC mandate M/436 (RFID)" SA/ETSI/ENTR/436/2009-02.

ETSI EN 300 220-1: "Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW; Part 1: Technical characteristics and test methods".

ETSI EN 300 330-1: "Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz; Part 1: Technical characteristics and test methods".

ETSI EN 302 208-1: "Electromagnetic compatibility and Radio spectrum Matters (ERM); Radio Frequency Identification Equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W; Part 1: Technical characteristics and test methods".

Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity (R&TTE Directive).

History

Document history		
V1.1.1	April 2011	Publication