PD CEN/TR 16670:2014

BSI Standards Publication

Information technology — RFID threat and vulnerability analysis

bsi.

...making excellence a habit.™

National foreword

This Published Document is the UK implementation of CEN/TR 16670:2014.

The UK participation in its preparation was entrusted to Technical Committee IST/34, Automatic identification and data capture techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2014

ISBN 978 0 580 83895 8
ICS 35.240.60

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 June 2014.

Amendments/corrigenda issued since publication

Date	Text affected

TECHNICAL REPORT

RAPPORT TECHNIQUE

TECHNISCHER BERICHT

CEN/TR 16670

June 2014

ICS 35.240.60

English Version

Information technology - RFID threat and vulnerability analysis

Technologies de l'information - RFID, analyse vulnérabilité et de menace

Informationstechnik - Analyse zur Bedrohung und Verletzlichkeit durch beziehungsweise von RFID

This Technical Report was approved by CEN on 20 January 2014. It has been drawn up by the Technical Committee CEN/TC 225.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

Foreword

This document (CEN/TR 16670:2014) has been prepared by Technical Committee CEN/TC 225 “AIDC Technologies”, the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This Technical Report is one of a series of related deliverables, which comprise mandate 436 Phase 2. The other deliverables are:

— EN 16570, *Information technology — Notification of RFID — The information sign and additional information to be provided by operators of RFID application systems*

— EN 16571, *Information technology — RFID privacy impact assessment process*

— EN 16656, *Information technology - Radio frequency identification for item management - RFID Emblem (*ISO/IEC 29160:2012*, modified)*

— CEN/TR 16684, *Information technology — Notification of RFID — Additional information to be provided by operators*

— CEN/TS 16685, *Information technology — Notification of RFID — The information sign to be displayed in areas where RFID interrogators are deployed*

— CEN/TR 16669, *Information technology — Device interface to support* ISO/IEC 18000-3

— CEN/TR 16671, *Information technology — Authorisation of mobile phones when used as RFID interrogators*

— CEN/TR 16672, *Information technology — Privacy capability features of current RFID technologies*

— CEN/TR 16673, *Information technology — RFID privacy impact assessment analysis for specific sectors*

— CEN/TR 16674, *Information technology — Analysis of privacy impact assessment methodologies relevant to RFID*

Introduction

In response to the growing deployment of RFID systems in Europe, the European Commission published in 2007 the Communication COM(2007) 96 'RFID in Europesteps towards a policy framework'. This Communication proposed steps which needed to be taken to reduce barriers to adoption of RFID whilst respecting the basic legal framework safeguarding fundamental values such as health, environment, data protection, privacy and security.

In December 2008, the European Commission addressed Mandate M/436 to CEN, CENELEC and ETSI in the field of ICT as applied to RFID systems. The Mandate M/436 was accepted by the ESOs in the first months of 2009. The Mandate addresses the data protection, privacy and information aspects of RFID, and is being executed in two phases. Phase 1, completed in May 2011, identified the work needed to produce a complete framework of future RFID standards. The Phase 1 results are contained in the ETSI Technical Report TR 187 020, which was published in May 2011.

Phase 2 is concerned with the execution of the standardization work programme identified in the first phase.

This document will provide the additional information of the RFID application that will need to be provided to a citizen by accessing the source identified on the sign where the RFID application is operating. This information will be aligned with the details set out in the Recommendation, but some of this might not be available at the outset, a Technical Report is the preferred form of initial delivery to establish basic requirements.

1 Scope

The scope of the Technical Report is to consider the threats and vulnerabilities associated with specific characteristics of RFID technology in a system comprising:

— the air interface protocol covering all the common frequencies;

— the tag including model variants within a technology;

— the interrogator features for processing the air interface;

— the interrogator interface to the application.

The Technical Report addresses specific RFID technologies as defined by their air interface specifications. The threats, vulnerabilities, and mitigating methods are presented as a toolkit, enabling the specific characteristics of the RFID technology being used in an application to be taken into consideration. While the focus is on specifications that are standardized, the feature analysis can also be applied to proprietary RFID technologies. This should be possible because some features are common to more than one standardized technology, and it should be possible to map these to proprietary technologies.

Although this Technical Report may be used by any operator, even for a small system, the technical details are better considered by others. In particular the document should be a tool used by RFID system integrators, to improve security aspects using a privacy by design approach. As such it is also highly relevant to operators that are not SME's, and to industry bodies representing SME members.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
blocker tag
tag forcing the reader to enter in its singulation algorithm

Note 1 to entry: The idea of the blocker tag that looks like a tag that we can have in our pocket, is to emit both '0' and '1' creating a collision and forcing the reader to enter in its singulation algorithm. If the blocker tag emits simultaneously '0' and '1' (that requires two antennas), the reader may never complete its algorithm. The blocker tag should be seen as a hacker device that is able to generate a denial of service in a legitimate system. We can even assess that a blocker tag has always a malicious behaviour since it cannot be selective and forbids the reading of one tag whereas it authorises the reading of the others. Moreover, the blocker tag works like a tag in a passive mode. So, it requires being in the reader field and it will protect only a small volume around itself. So a blocker tag can be considered as a malicious tag, which prevents a legal system to read legal tags or as a mitigation technique preventing an illegal reader to read a legal tag.

2.2
blocking
another way to produce a denial of service is to interfere during the anti-collision sequence

Note 1 to entry: Different devices have been developed.

2.3
cloning
impersonation technique that is used to duplicate data from one tag to another

Note 1 to entry: Data acquired from the tag by whatever means is written to another tag. Unless the technology and application require the interrogator to authenticate the RFID tag, cloning is possible. Cloning the unique chip ID presents a significantly bigger challenge for the attacker, but some researchers claim that this is possible. There is also a special case of cloning that needs to be considered where the application accepts multiple AIDC technologies. Cloning data from an RFID-enabled card can be replicated in magnetic stripe. In some payment card systems, information that might be

cloned from an AIDC card could be used in payment situations known as 'cardholder not present' for purchases made on the Internet or by telephone. In this case, the clone is virtual and requires no encoding on another RFID tag.

2.4
denial of service
preventing communication between the interrogator and the tags

Note 1 to entry: There are two main ways to accomplish a "denial of service". The first one is to create electromagnetic interferences, the second one is to insert a blocker tag in the communication.

2.5
destruction
making the tag definitively unusable without using a logical kill function whenever such a function exist in the rfid protocol

Note 1 to entry: Destruction may refer to the reader too. Although this attack threats RFID system availability, it's different from deny of service because it can't reactivate and repair it. Destruction is considered as an attack when it's practiced without holder's knowledge. Two destruction types can be distinguished1) Hardware-and 2) Software destruction. While this can be seen as a security threat to the RFID operator, there are also situations where it might affect the individual. For example, if a public transport tag is accidentally damaged, then the individual's rights associated with it can be lost. In a similar manner as for tag removal, tag destruction can be used as a control to protect the privacy

2.6
eavesdropping
passive attack, which consists in remotely listening to transactions between a Real Reader and a Real Tag

2.7
guardian
special device developed by Melanie Rieback from a Dutch University to help citizens to communicate with their own contactless smartcards

Note 1 to entry: As an active device it can be turned into a blocking tag preventing an attacker to access such contactless cards. Thus, it can blur any pervasive reading by actively emitting a jamming signal in the sidebands of a typical RFID tag. Such a mechanism enables multiple functionalities:

— information can be sent to the reader or to the tag for secret key management, authentication, access control;

— monitoring of the RFID environment to warn of possible unsolicited reading;

— creation of collisions to prevent from the possible inquisitive reading.

As a consequence, the RFID guardian is a useful tool to ensure the privacy but it is also an efficient device to create denials of service. Whereas the blocker tag is designed to carry out a simple load modulation, the RFID guardian is an active device that requires batteries and that is able to emit is own signal. As a consequence, the distance of use is much larger.

2.8
jamming
creating a signal in the same range as used by the reader in order to prevent tags from communicating with the reader

Note 1 to entry: Because the RFID air interface protocol depends on radio signals, an attacker can exploit any such signals within the range of the communication between interrogator and tag

2.9
man in the middle
object or person interfering in the communication between a real reader and a real tag

Note 1 to entry: "Man in the middle" attack is often mistaken for relay attack. These are indeed similar but with the distinctive feature that in this attack the bit stream can be modified in the relay. Since the relay implies the adaptation of the modulation and of the bit coding by the Fake Reader or the Fake Tag for its use, it is not a problem to change some bits. This additional feature may take time but it will always be shorter than the timeout of the Real Reader.

2.10
RFID (1)
radio frequency identification
use of electromagnetic or inductive coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to uniquely read the identity of an RF Tag

[SOURCE: ISO/IEC 19762-3]

2.11
RFID (2)
radio frequency identification
use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to uniquely read the identity of a radio frequency tag or other data stored on it

[SOURCE: RFID Recommendation C(2009) 3200 final]

2.12
relay attack
kind of Man in the Middle attack where fake reader and fake tag are used

Note 1 to entry: The relay attack is based on a specific weakness of the RFID tags that has the possibility to activate the device without the consent of the user. Indeed, a user is not able to switch off his tag. Thus an attacker can, therefore, access the tag discreetly, without knowledge of its owner, and relay information through a communication link between the tag and a remote Fake Reader. The reader will assume that the tag, and by implication the user, is in close vicinity and provides access to the attacker. Using this attack on cryptographic authentication schemes, the attacker would be able to convince both Real Reader and Real Tag to share a common secret key. The attacker would not be able to view in plaintext any subsequent communications. This is not needed as long as it can continue relaying the respective messages. The attack can be given an active twist by relaying the initial authentication sequence after which subsequent data is modified and relayed. Relay attacks involve two different devices and as a consequence two attackers that should coordinate each other except if the relay is really short (an arm's length for example). The device that will skim the data of the attacked person is the Fake Reader. The Fake Reader is linked via the relay to the Fake Tag, a Fake Tag that will reproduce the data of the Real Tag.

2.13
side channel analysis
analysis which allows to find secret information by using the analysis of the RF field during the processes made by the tag processor

2.14
side channel attack
attack which uses a Side Channel Analysis

Note 1 to entry: In a side channel attack, the information that is usually exploited includes timing information, power consumption or even electro-magnetic fields. This type of attack requires sufficient time, specialist equipment, and deep knowledge of the internal systems on which the cryptographic and other algorithms are implemented.

2.15
singulation
identifying an individual tag in a multiple-tag environment

2.16
skimming
active attack which consists in reading a tag

Note 1 to entry: It includes powering and modulation. It implies distance tag activation without consent of the operator of the application.

2.17
substitution
action of changing a real reader or tag by a fake one

Note 1 to entry: There are two kinds of substitution:

— Reader substitution: Reader substitution is a kind of smart jamming. During such an attack a Fake Reader radiates a RF magnetic field in order to perturb a communication between a Real Reader and a Real Tag. The goal of this perturbation is not to entirely block the communication but to transform the initial reader's message to access forbidden zones of the tag memory or to induce misusing of the tag. Depending of the goal of the attacker, all Real Reader's messages can be transformed or some messages can be kept unchanged (during initialisation protocol or Real Tag's authentication for example). A way of setting up such an attack is to make the Fake Reader speak louder than the Real Reader. This can be easily done if the Real Reader is far from the tag. The Fake Reader attacker has only to be nearer than the Real Reader. This attack is very complex to set up.

— Tag substitution: Tag substitution cannot be performed in the same way as reader substitution. Indeed, the attacker's tag cannot "speak" louder than the official Real Tag. The attacker has to use a powered RF device near the Real Reader and Real Tag to create a RF signal. This signal can then be superimposed on the official backscattered signal from the Real Tag leading to the cancellation of this signal from the Real Reader's point of view.

2.18
tag
RFID device having the ability to produce a radio signal or a RFID device which re-couples, back- scatters or reflects (depending on the type of device) and modulates a carrier signal received from a reader or writer

[SOURCE: RFID Recommendation C(2009) 3200]

2.19
tag cloning
action of taking information from a real tag to create a fake tag with same functionalities

2.20
truncation
action of shortening (a number or a word) by dropping one or more digits or bits

3 Symbols and abbreviations

ALOHA	Probabilistic algorithm used for RFID tag singulation.
CCTV	Closed Circuit Television
CSP	Communications Service Provider
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
DPP	Data Protection and Privacy
EAS	Electronic Article Surveillance
EPC	Electronic Product Code
ESO	European Standard Organisation
ETSI	European Telecommunication Standard Institute

FR	Fake Reader

NOTE 1 The reader used for the attack and not part of the application.

FT	Fake Tag

NOTE 2 The tag used for the attack and not part of the application.

HF	High Frequency
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISO	International Standard Organization
LF	Low Frequency
OCR-B	Optical Character Recognition type B (cf. ISO 1073-2).
PIA	Privacy Impact Assessment
RFID	Radio Frequency Identification
RR	Real Reader

NOTE 3 The reader used in the application.

RT	Real Tag

NOTE 4…The tag used in the application.

SIM	Subscriber Identification Module
SME	Small and Medium Enterprise
STF	ETSI Special Task Force
TID	Tag IDentifier
UHF	Ultra High Frequency
UII	Unique Item Identifier
UWB	Ultra Wide Band
WLAN	Wireless Local Area Network

4 Threats and Attack scenarios

4.1 Introduction

This clause analyses the various combinations of attacks to a RFID system comprising a RR and a RT, with the help of a FR, or a FT, or both a FR and a FT. Figure 1 summarises the combination of different readers and tags for a given attack.

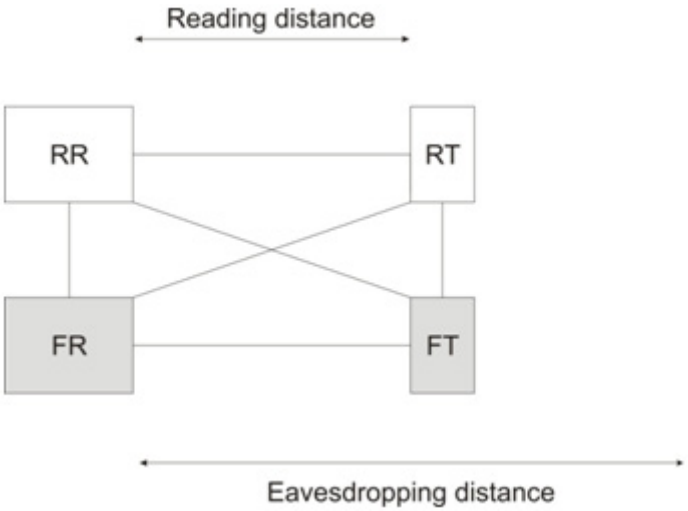

Figure 1 — Penetration Testing Framework: a proposed pictorial representation

4.2 Attacks to an RFID System with a Fake Reader

Three RFID devices are operating at the same time: RR + RT + FR.

A Fake Reader operating within the range of a RFID application, can perform two types of attacks:

— By generating radio waves at the same wavelength of the application it can generate interference with the application communication sequences, if sufficient energy is deployed (field strength in the vicinity of the RR). This prevents the exchange of data between RR and RT, and creates a denial of service.

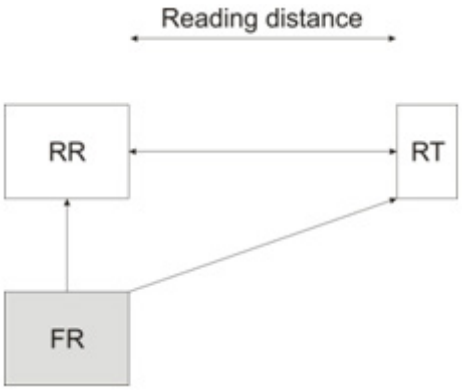

Figure 2 — FR used as interferer

— The reader can also listen (record the variation of the amplitude or the frequency during the communication) to the RF communication of the real RFID application. The FR is eavesdropping on the RFID application.

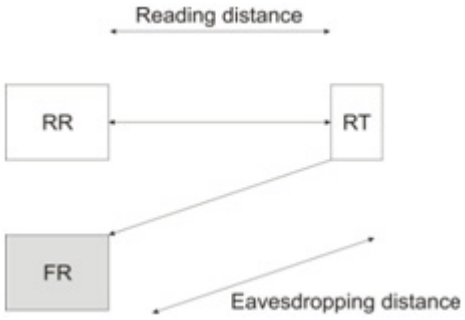

Figure 3 — FR used to eavesdrop RT's signal

NOTE An attack performed by a Fake Reader is not possible if there is no Real Tag in the environment, since a Real Reader will not respond to a Fake Reader.

4.3 Attacks to a RFID system with a Fake Tag

Three RFID devices are operating at the same time: RR + RT + FT.

If the FT talks to the RR at the same time then the RT, the RR will not determine which of the two tags will send the correct information creating a denial of service.

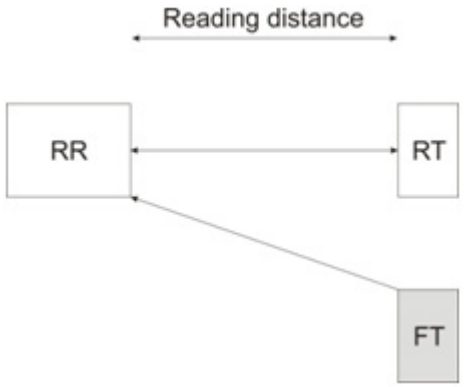

Figure 4 — Attack performed by a FT

NOTE An attack performed by a Fake Tag alone will be inoperative if there is no Real Reader in the environment, since no communication can exist between two tags.

4.4 Attacks to a RFID system with a Fake Reader and a Fake Tag

Four RFID devices are operating at the same time: RR + RT + FR + FT.

In this scenario, two attacks can be performed at the same time or independently:

— RT is activated by FR. FR writes the information collected from RT into FT creating a cloned tag;

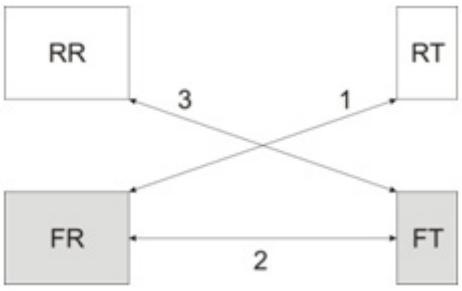

Figure 5 — Creating a cloned tag

— FT is activated by RR and responds with its own fake data creating a Man in the Middle attack.

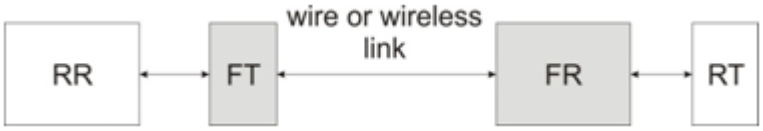

Figure 6 — Relay attack

4.5 Attack to a Real Tag with a Fake Reader and a Fake Tag

Since there is no communication possible between two tags, the attack can be performed only by the Fake Reader. See 4.6.

4.6 Attack to a Real Tag with a Fake Reader

A Fake Reader activates a Real Tag and writes new information in the Real Tag creating an **unwanted tag activation.** Real data may be modified without consent.

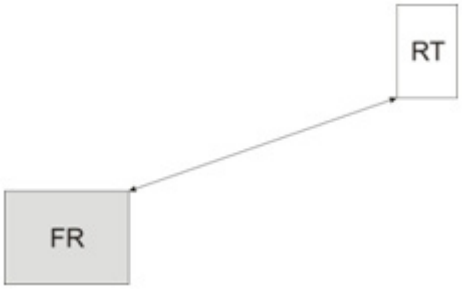

Figure 7 — Unauthorised tag activation

We can dissociate the activation side of the attack from the listening side. In that case, we need a first fake reader which only purpose is to activate the tag by sending it a transmitting signal. Another fake reader can be placed farther away just to eavesdrop the backscattered signal from the real tag. The spatial limitation of such an attack is given by the activation range. Some commercial systems make use of this approach by using different activation points to "illuminate" a wide area and place only one receiver to collect all the tags' responses. Special signal processing is set up to recover the antenna which activates the tag and therefore performs localisation.

4.7 Attack to a Real Reader with a Fake Tag

The Fake Tag can send false information to the Real Reader. The consequence can be similar to the case of an unwanted activation.

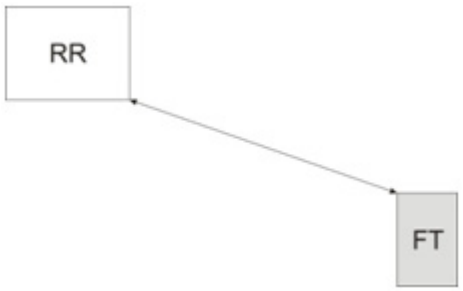

Figure 8 — Use of unauthorised tag with Real Reader

5 Vulnerabilities

5.1 Introduction

All attacks are made while listening to and/or activating the communication between the Real Reader and/or the Real Tag. In all cases, the attacking devices must operate at the same frequency as the victim.

The vulnerabilities are to the reader, tag or Air Interface Protocol depending on the type of attack.

At the reader level, the Real Reader cannot differentiate between the Real Tag and the Fake Tag. At the tag level, the Real Tag cannot differentiate between the Real Reader and the Fake Reader.

At the Air Interface Protocol level, the vulnerability comes from the fact that the communication between the Real Reader and the Real Tag is normally understandable, deterministic and sequenced. Thus leaving space and time to intervene in the communication with fake devices.

— Understandable: commands and answers can be identified and copied enabling fabrication of Fake Readers and Fake Tags capable of communicating with Real Readers and Real Tags. Where this is applied it enables unwanted data capture or sending wrong information or creating interference and noise to provoke denial of service;

— Deterministic: commands and answers are always the same in the protocol, thus enabling unwanted activation and therefore unauthorised identification of personal data and/or data linked with individuals;

— Sequenced: the timing for questions and answers is sequenced. When the sequence is long or if there is no sequencing, it leaves enough time for an attacking system (Fake Reader and Fake Tag) to attack through man in the middle.

5.2 Denial of service

This attack can be made either by a Fake Reader or by a Fake Tag. The vulnerability is located in the air interface protocol and at the reader level.

5.3 Eavesdropping

This attack can be made by a Fake Reader. The vulnerability is at the Real Reader, Real Tag and Air Interface Protocol level.

NOTE Listening to the communication between a tag and a reader by scrutinising small signal variations on device's power line supply cannot be associated with eavesdropping. Such an attack can be classified in the side channel attack of the system and is not specific to RFID.

5.4 Man in the Middle

This attack needs a Fake Reader associated with a Fake Tag. The vulnerability is in the Air Interface Protocol.

6 Mitigation measures

6.1 Introduction

The measures depend on the RFID technology used. There are several standardised Air Interface Protocols used in each frequency range and many non-standardized protocols being used in existing RFID applications.

6.2 Mitigation measures for secured RFID Devices

6.2.1 Mitigation measures for tags

— authentication of tags;

— special command for the TID enabling comparison to a pre established list;

— encryption of data.

6.2.2 Mitigation measures for readers

— authentication of tags.

6.2.3 Mitigation measures for the Air Interface Protocol

— no personal data;

— encryption of data;

— no TID;

— truncated UII/EPC codes;

— reduced reading range.

6.3 Mitigation measures against attacks

6.3.1 Introduction

This subclause lists solutions against the following types of attacks.

6.3.2 Eavesdropping

The main solution to eavesdropping attacks is the encryption of the data and the use of cryptographic signatures. Symmetric keys, and asymmetric keys can be used. However, those algorithms require a lot of computing resources which could be too large for RFID tags in certain applications.

6.3.3 Skimming

There are several measures to avoid skimming of contactless cards:

Optical reading: To avoid skimming of contactless cards, a solution was developed for and applied in the electronic passport. This is the association of an optical reading with the contactless reading of the device often linked with symmetric algorithms. Only the optically read data on the two dimensional barcode of the passport enables the access to the contactless chip. A main weakness of this countermeasure is that a

barcode or OCR-B can be easily counterfeited. As a consequence, a passport should not be opened and showed to anyone else but the authorities. This condition is difficult to enforce as everybody knows that his passport could be looked at the desk when checking in a hotel.

The Faraday cage*:* Another basic solution is to confine the tag or the contactless card in a wallet made of a metallic sheet or mesh. This wallet is acting as a Faraday cage blocking the HF and UHF radio signals of readers. The efficiency is certain but the use is restraint.

6.3.4 Relay attack

A mitigation technique to reduce relay attack risk on classic RFID channel (narrow band communication) is to use another channel to send very short pulses (time domain). For a given distance range, time of flight (time between reader command and tag response) for such short pulses are well known so that if relay attack occurs, time of flight will be much greater than that expected resulting in a code violation (error) in the second encrypted channel. Knowing that real reader and real tag can infer that man in the middle attack occurs and can decide to stop the data transmission.

The data channel does not change (still classical HF or UHF narrow band signals can be used) but a second channel (UWB like) is needed to share the value of the time of flight between reader and tag.

6.3.5 Denial of Service

A number of techniques exist to prevent operation of a RFID system.

The active jamming*:* It is possible to create a device that emits signals at the same frequency as the Real Reader to jam its communications with the Real Tag. A lot of denial of service attacks could be seen also as a more or less efficient countermeasure. This device should broadcast signals at higher powers than the different standards permit and as a consequence it is illegal.

The blocker tag**:** This device is mentioned in previous subclauses since it can be seen also seen as an attack tool. The main drawbacks of the blocker tag are that it cannot be selective (it will blur a family of tags) and that it is a passive device that requires activation by the Fake Reader to work.

The RFID Guardian**:** This device is also aforementioned in the denial of service attack. It enables a large panel of services to protect the user: secret key management, authentication, access control, monitoring of the tag environment, creation of collisions. It does not have the main drawbacks of the blocker tag since it can be active. Nevertheless, the selectivity can only be reached with an ALOHA type anti collision protocol and this is not a multi - standards solution.

7 Conclusions

It is worth pointing out the tremendous richness of the hackers' imagination and the profusion of concepts designed to jeopardise the contactless link. It is therefore important to stay informed of any new potential threats. Of course this kind of "sporting" activity is not specific to contactless smartcard technology.

During the risk analysis process required for a PIA, the operator will have to quantify the scale of risk associated with the various threats. In order to do that the RFID operator can use the results of this Technical Report and, some complementary experiments may be undertaken to assess the technical possibilities of each specific attack and to measure the associated risk numerically.

Finally, because hacking is an endless human activity, a continuous survey of new attacks must be performed through published technical papers, hackers' websites and unofficial workshops.

In all cases, the threats can be real if carried out within the read and/or write range of each of the RFID technologies used in a given RFID application.

A lot of articles have been published quoting actual read and/or write ranges at each of the frequencies and protocols used by RFID. Metrics covering such ranges is part of this Technical Report and are included in Annexes B and C.

In order to assess the level of risk associated with the different threats identified in this document, a series of tests were performed during Phase 1 of the mandate M436 and have been published under an ETSI Technical Report referenced TR 101 543. The document is listed in the bibliography and relevant extracts are included in Annex B.

Additional tests have been performed during Phase 2 covering other frequencies used in the main applications like retail and libraries. A summary of the conclusion is given in Annex C. These tests were performed on 26-27 November 2012 at Nedap.

When considering the threats to an installation, it will be important for system integrators and end users to strike a balance between the effort and risk of attacking a RFID system and the perceived benefit to the attacker. The results of the practical tests documented in Annex C provide some useful guidelines when carrying out such an assessment

Annex A
(informative)

Attack scenarios

A.1 Amusement parks takes visitors to RFID-land

A.1.1 Introduction

A European theme park is helping parents keep track of their children by giving them RFID embedded wristbands embedded. The RFID wristband is issued to all visitors at the park entrance as part of general admission to the park.

The wristbands contain special microchips, or RFID tags, that wirelessly signal their whereabouts to reading devices throughout the park facility. Visitors can locate other members of their group by using touch-screen kiosks located at strategic places within the park boundaries. The kiosks are linked to a real-time locating system, including the visitor's ticketing database. The system combines passive and active RFID tags and readers.

The watch-like plastic bracelet, which holds the active RFID chip, transmits a signal every 12 to 15 s and there are 25 RF readers that continuously search for the signal from the tags as visitors walk though the various playgrounds and facilities in the parks aqua splash. Each antenna creates its own zone and most zones in the park are about 300 meters.

The system is PC-based connected with fibre network to the back-end servers (database and application servers). The park thus far only uses the system for location services, but it is possible to configure the software to end an email alert of the person wearing the bracelet wanders outside of the radius the readers can detect.

The bracelets with the RFID tag is for rent and is shall be handed in upon park exit. In cases where the bracelets is lost or not handed in, a fine must be paid.

This threat scenario exploration will focus on two sub scenarios. In the first sub scenario the bracelet is return upon exit, while in the second sub scenario the bracelet is still with the child after leaving the park.

A.1.2 Threat scenarios

Attackers manage to bring Fake Readers into the park and place these unnoticed at several locations throughout the park. The readers are equipped with WLAN enabled SIM cards, regularly sending readings to the attackers computers. These computers are connected to the Internet and are able to deduce the name of both children and parents by linking the tag identity with information on the children and parents kept at the parks location database, which the attackers have hacked into. The attackers are further able to deduce the home address and phone number of the parents and their children.

This is a violation of the privacy of the tag bearer and other individuals associated with the tag in the location database. The aggregation of tag identity and personal information from the database makes the attacker able to place a RF reader within the perimeter of the home of families still in possession of the RFID embedded bracelet. As name and phone number of one of the parents and the name of the child is registered upon tag rental, the attacker can easily deduce the home address and other personal information. The Fake Readers can also be used to aggregate behavioural information of the child, as the location of the Fake Readers are placed at known locations and close to attractions.

The Fake Readers are also able to successfully block the RF interface between legal RF readers and RFID embedded bracelets. Other Denial of service attacks are also possible and can be executed from the Internet or the mobile network, as the fake RF readers are equipped with WLAN enabled SIM cards. The attackers can either send messages to the SIM card using messaging services or connect to the reader via the WLAN antenna of the SIM card. 7

Attacker hacks into the database keeping track of visitors not having returned the bracelet upon park exit. For some reason the parents cannot find the bracelet when leaving the park, even though it is still in their possession (the child has managed to remove the bracelet and put it in his mothers bag). The attacker searches the database and extracts the name of the parents not returning the tag. They then manage to gather information on home address and phone numbers. The mother still has the tag in her bag, enabling the attacker to place readers in the vicinity of her home. The RF reader using the embedded SIM card to sends a message to the attacks cell phone every time the tag is read. Personal information in the location database can be used to deduce home address and to track the families' movements even after leaving the park. The SIM card enables tracking and aggregation of behavioural information if several Fake Readers are placed for example around a particular city.

With the knowledge of which visitors did not hand in the bracelet upon park exit, theft of the bracelet outside the park boundaries are made possible. This can also be used to study the bracelet enabling cloning of credentials and tags, but also illicit access to data and other unauthorised access and manipulation of the data on the bracelet.

The fake RF readers may also be able to distribute worms, viruses and malicious code if they manage to connect these to the fibre network in the park or via a potential wireless network within the park.

A.1.3 DPP objectives of relevance

— Personal data should be collected by legitimate parties only; Personal data should be collected by legitimate means only; Personal data should be stored by legitimate parties only; Personal data should be processed by legitimate parties only

— A CSP should clearly specify the start and end of data collection purpose;

— RFID purpose of use categories should identify the required actions of operators and control measures involved; CSP operators should specify as a minimum: start of purpose, purpose of data collection, end of purpose and permissions;

— Personal data should only be processed according to the purpose(s) of the collection;

— Personal data should be rendered anonymous, e.g. using pseudonymous data, whenever processed or stored; Personal data should only be processed according to the purpose(s) of the collection;

— CSP operators should embed a feature into the tag that will erase or scramble the item serial number and let only the item class type description completely or partially available (the contrary is also possible but with different privacy implications);

— Individuals should be able to disable ("silence of the chips") the content of RFID tags in a manner that does not penalise that particular individual in any way;

A.1.4 Security objectives of relevance

— Personal information, behaviour-related information and possessions RFID tags should not be revealed to any party not authorised to receive the information.

— Personal information collected by RFID tags should be collected by legitimate means only.

— Personal information sent to or from any component in the RFID ecosystem should not be revealed to any party not legitimate to receive the information.

— Personal information held within one or more components of the RFID ecosystem (RFID device, tag, reader, network connections, backend systems) should be protected from non-legitimate access from outside of the RFID ecosystem.

— The identity of a user should not be compromised by any action of the system.

— No action of the system should make a user liable to be the target of identity crime.

A.1.5 Privacy objectives of relevance

— Individuals should be protected against profiling (linking of name and other private information, location of that particular person and activities being performed by the person)

— Location information contained on RFID tags should only be accessible to legitimate parties when in possession of individuals

— Location information contained on RFID tags should only be accessible by legitimate means when in possession of individuals

— In cases where personal data, behavioural data or data that can be used to link the content of the tag to a person, the item identity shall be rendered anonymous using pseudonyms

A.2 Purpose of Use and Consent

A.2.1 Purpose 1

Mrs Berglund is shopping in a branch of the department store Sokos in Helsinki. She has purchased a number of items for the kitchen and also a pair of Nike trainers for her 13 year old son. All items are RFID tagged for security purposes on behalf of the store to avoid theft and for logistic reasons and because the store follows the European recommendation to disable or remove tags before the consumer leaves the store, all tags shall be disabled or removed at point of sale (or check-out).

NOTE We are here envisioning a European recommendation to disable or remove tags upon check-out or point of sale.

All the kitchen item tags are disabled according to the European recommendation having fulfilled their security purpose in the store. However, the tag incorporated into the trainers is not disabled since Mrs Berglund explicitly agrees to the Nike promotion linked to this new product. In fact the Nike promotion has prompted the purchase as her son heard about it and requested Nike trainers for this reason.

Figure A.1 — Athletic shoe

Mrs Berglund continues shopping that day in other stores with RFID security.

A.2.2 Purpose 2 (with explicit consent)

The Nike offer is the first of many it hopes to run across Europe. The promotion is currently confined to Finland. The offer is for owners of the new trainers to participate in a game undertaken in the vicinity of Helsinki. Some 20 RFID readers are distributed around retail environments in the city and the readers are linked to co-located personal computers and hence screens. The Nike marketing people call these “Customer Interaction Stations”. The players interact with the stations when the Nike trainers they are wearing are detected by the readers, thereby triggering, on the associated screens, an anonymous invitation to play.

Local businesses are involved in the Nike promotional game as well as McDonalds, Apple and Benecol.

The game takes the trainer wearers round the city to undertake various tasks and at a higher level of the game it involves interaction with other players both within the virtual element of the game and in the physical world too. Higher level players register providing personal details as well as pseudonyms to be utilised by within the game.

A.2.3 Purpose 3 (with no explicit consent

A year later Mrs Berglund’s son, wearing his trainers, is on a school trip to Paris when on passing a shoe shop an advertising screen displays his name and offers him discounted tickets at a local cinema if he purchases a new pair of shoes. Neither he nor his mother has given consent for anything like this.

Figure A.2 — Screens

A.3 Multi-tag and purpose RFID environment for Healthcare

A.3.1 Scenario description - Emergency

Mr Smith, a 70-year-old British grandfather, is visiting the South of France with his children and grandchildren for a family holiday. Mr Smith had a heart attack some years ago and now wears a pacemaker. In the middle of playing a game with the grandchildren he collapses gasping for breath and his daughter calls the French emergency services who arrive in minutes.

Mr Smith is rushed to hospital unconscious.

A.3.2 The hospital RFID environment

The hospital is on the front-end of applying RFID technology to ensure effective and correct care services. The hospital is among the top-ten in Europe. There are over 50 applications enabling RFID technology in the hospital, covering bed and asset management, equipment maintenance, patient and staff safety, patient flow, infection tracking and control, and drugs dispensing. The medical equipment incorporated in the hospital's RFID system is the best, coming mainly from France, Germany, Italy and Switzerland.

A Norwegian System Integration company provides the RFID system design control and integration. The system operation and maintenance is outsourced to the French arm of an American company while the RFID system elements such as readers and applications come from France, Belgium, USA, India and Spain

Figure A.3 — RFID enabled Bed

Tagged items range from bed sheets and medical instruments (asset management and infection control applications) to passes for staff and drug containers for security and operational monitoring. The tags entering the hospital's RFID environment have different suppliers, mainly American, European and Chinese. Over 300,000 individual tags per annum legitimately interacted with 50+ applications using 500 fixed and hand held readers. Over a million tags pass by the hospital's readers' each year.

A.3.3 Arrival at the hospital

Mr Smith's RFID'ed passport is utilised by his family for a rapid check of his European credentials and rights to free care.

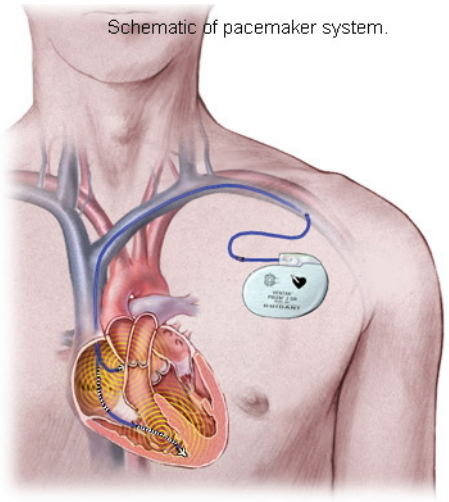

Figure A.4 — Implanted Pacemaker

Mr Smith also carries an RFID card which automatically identifies that he is wearing a pacemaker

A.3.4 Treatment at the hospital

Mr Smith is rapidly diagnosed as having a complication with his heart and lungs, which can be easily managed with a recently developed American drug. He is required to stay in the hospital for a two-day observation and to bring the recent additional condition under control. When his drugs are prescribed, allowance is made for his return trip to the UK and special notice of the need to make additional arrangements for further supply of the drug (which is not widely used in the UK) when returning to the UK. He is given a month's supply of the drug, which is held in an RFID labelled container, used within the hospital's dispensing system.

A.3.5 The value of the drug prescribed

The drug that Mr Smith is now using to control his new medical condition has, in the last year, become a key part of an illegal cocktail hitting the drugs scene. The drug is not common and the value 'on the street' is high making it a target for theft. The many supply chains for this particular drug use a wide variety of tags and criminals have "acquired" the EPC records relevant to the drug.

Clandestine readers are known to be 'on the street' to help thieves detect the presence of this criminally desirable drug.

A.3.6 Returning home

When Mr Smith returns home he registers his new drugs into his "smart medicine cabinet" used to keep both his and his wife's medications. The cabinet uses RFID and runs its associated applications on the family personal computer along with other RFID applications, some of which are accessible remotely by commercial companies and some applications which are accessible remotely by family members.

Figure A.5 — Drugs cabinet

A.3.7 The home RFID environment

Thanks to Mr Smith's son in law's enthusiasm, Mr Smith's home has 4 low cost multipurpose RFID readers providing drug monitoring, house security, energy use by appliances, washing machine programme control, entertainment and games and occupant activity monitoring so the Smith's daughter can keep a discrete eye on her parents. The house has over 200 tagged items legitimately interacting with its small RFID system.

A.3.8 Drug repeat prescription and out of date drug recycling

Mr Smith's local General Practitioner (GP) Surgery (a group of 20 GP's) has introduced a system of repeat prescription and old drug removal through the presentation of the RFID tagged and or bar coded drug containers at the surgery. When drugs are out of date the surgery takes them in for disposal.

Figure A.6— Out of date drugs

The UK National Health Service (NHS) using outsourced installation and maintenance teams provides the GP's RFID system. There are 20 RFID applications in the Surgery and with over 20,000 patients to look after there are more than 10k tagged items on the system, all moving in and out of the surgery following patients and carers. The number of tagged items is expected to become 40k within a short period of time. The local processing is managed and operated directly by the surgery staff while the system interfaces to the main NHS systems for patient data sharing for a number of detailed NHS purposes.

Annex B

Original Test Set ups and Results

B.1 Test Area

All the majority tests were performed in the meeting area at the N.V. Nederlandsche Apparatenfabriek “Nedap” premises in Groenlo, The Netherlands.

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.

B.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 x 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 – 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.

B.3 Overview of the Tests

B.3.1 Introduction

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

B.3.2 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 battery less (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.

B.3.3 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.

B.3.4 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 (eg 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.

B.3.5 Eavesdropping

Some members of the STF had expressed concern about the ability of a person with criminal intent to monitor remotely the response from a tag while an interrogator was reading it. 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.

B.3.6 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.

B.3.7 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.

B.4 Test procedures and results

B.4.1 General

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 in Table B.1 here below

Table B.1 — Measurements of noise floor levels

Frequency range system	Measuring frequency range	Measuring Band width	System Band width	Noise Measurements in dBµV/m Unless otherwise noted			Type of noise and source	Source
		kHz	kHz	1	2	3		
LF Nedap (kHz)	116-119,5	0,150	2	41	43	41	Broadband	External
	120,0	0,150		98	82	85	Unmodulated Carrier	Neighbouring Nedap systems
	120,5-124	0,150	2	41	41	54	Broadband	External
LF TI (kHz)	124-138	0,150	2	46	51	61	Broadband	External
	129	0,150		60		58	Radio Signal	External
	135	9			48		Radio Signal	External
HF Mifare (MHz)	12,64-12,79	9	150	<36*	42		Broadband	External
	12,64-12,71	9			45		Small band RFI	Battery charge
	14,33-14,48	9	150	<36*	<36*	<36*	Broadband	External
	14,36-14,43	9			42		Small band RFI	Battery charge
	12,72	9		32			Radio Signal	External
HF Vicinity (MHz)	13,11-13,16	9	50	<31,5*	34,5	35,5	Broadband	External
	13,17	9			47		Small band RFI	Battery charge
	13,95-14,01	9	50	<31,5*	<31,5*	<31,5*	Broadband	External
	13,96	9			35		Small band RFI	Battery charge
UHF (MHz)	865-868	150	150	-104 dBm	-	-104 dBm	Broadband	Noise floor measuring receiver
	865,7; 866,3 866,9; 867,5	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 power in the system bandwidth								
Noise measurement 1 is performed on Monday 6th, 2010 before start of the tests Noise measurement 1 is performed on Monday 6th September 2010 after the tests Noise measurement 1 is performed on Tuesday 7th September 2010 before the start of the tests								

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.

B.4.2 Reading range

B.4.2.1 Introduction

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.

B.4.2.2 Reading range for LF systems

A loop antenna of approximate dimensions 40 x 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 µA/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 B.1 — Measuring reading range at LF below.

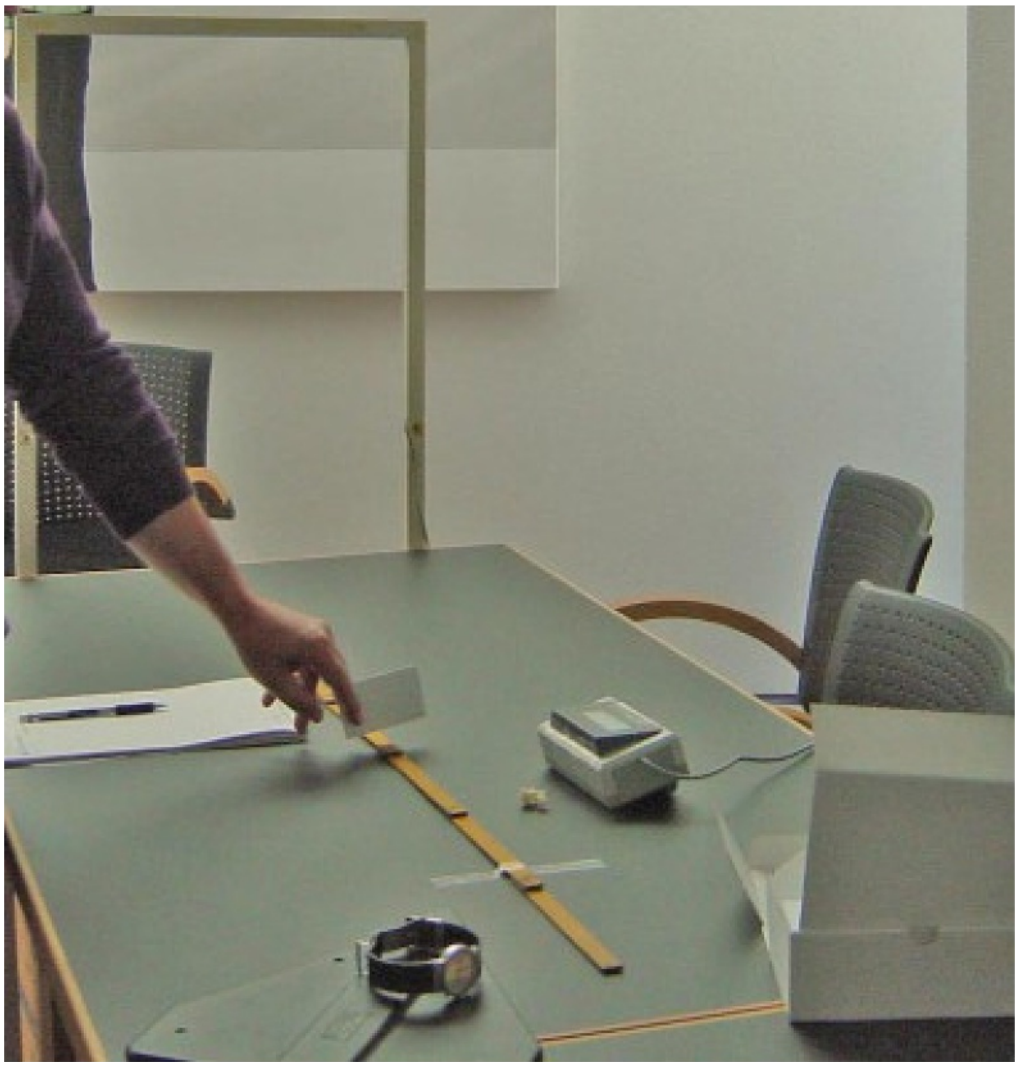

Figure B.1 — Measuring reading range at LF

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 B.2.

Table B.2 — 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 %		Upper		90,81	91,98
			of tags will fall between		Lower		83,53	86,87

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.

B.4.2.3 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 dBμA/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 B.2 — Measuring reading range at HF.

Figure B.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 B.3.

Table B.3 — 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 %			Upper	81,83	85,37
			of tags will fall between			Lower	78,64	78,03

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 and 78 cm.

B.4.2.4 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 B.3 — Measuring reading range at UHF.

Figure B.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 – 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 B.4

Table B.4 — Reading range results for UHF tags

Batch 1

Serial No.	1st measurement		2nd measurement		3rd Measurement		Mean range	
	In (m)	In (m)	In (m)	In (m)	In (m)	In (m)	In (m)	In (m)
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 %			Upper	3,69	3,72
				of tags will fall between			Lower	3,15	3,19

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.

Table B.5 — Reading range results of the latest integrated circuits manufactured by Impinj

UHF Tests

Serial No.	Max read range (m)
1	7,85
2	8,2
3	8,5
4	8,9
5	9,75
Arithmetic mean	8,64
Standard Deviation σ	0,73
Two standard deviations 2σ	1,46
Max write range of 95 % of tags	10,10
will fall between	7,18

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.

B.4.3 Write range

B.4.3.1 Introduction

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.

B.4.3.2 Write range at LF

These tests were performed using a purpose made writing unit. A picture of the equipment is shown in Figure B.4 — Measuring write range at LF.

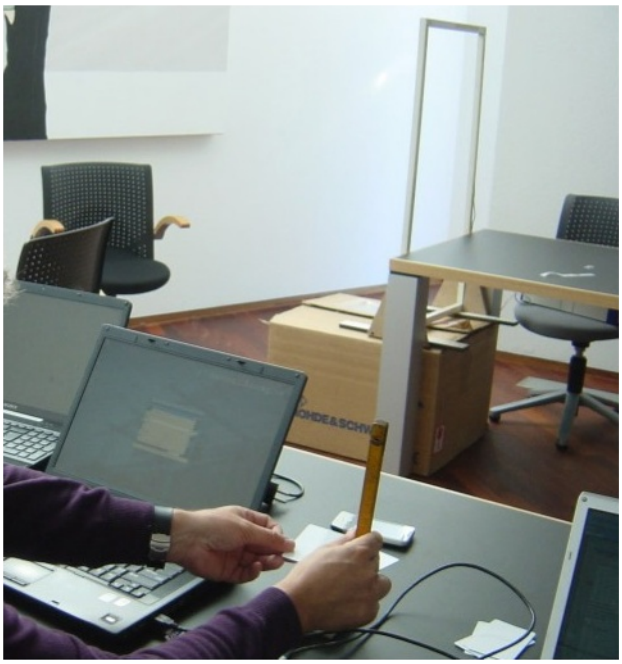

Figure B.4 — Measuring write range at LF

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 B.6 here below

Table B.6 — Tests results

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	6,39
will fall between	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	78,35
will fall between	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	10,10	9,40
will fall between	7,18	5,96

B.4.3.3 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 B.6.The typical maximum write range was 4,6 cm with no tag functioning above 6 cm.

B.4.3.4 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 B.6 here above.

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

B.4.3.5 Write range at UHF

Measurements of the write range at UHF were performed on a prototype interrogator. See Figure B.5 — Write range equipment at UHF.

Figure B.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 B.6, here above.

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 must 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 B.6, 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, the uPASS Reach interrogator had been received range limited and explained the reduced reading performance.

B.4.4 Illicit reading

B.4.4.1 Introduction

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.

B.4.4.2 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 B.6 — Contents of tagged items in shopping bag. The identity number of each of the tags was recorded.

Figure B.6 — Contents of tagged items in shopping bag

A handheld reader (Figure B.7 — Hand held reader) was used to simulate the illicit reading of the contents of the shopping bags.

NOTE It is recognized that a person with illicit intent might choose to use another device with different capabilities.

Figure B.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 B.7 here below.

Table B.7 — Analysis of illicit reading of shopping bags

Serial No	Tag number	Colour of bag
1	AD99210442528F92600000DF	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	AD99210442527B92600000DD	O
11	AD9921044251E391630000CB	W
12	AD9921044252979061000E0	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. It is recognised that by repeatedly reading the bag carried by a person, it might eventually be possible to deduce its contents

B.4.4.3 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 B.8 — Tagged bottles and box of pills.

Figure B.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 and 90 cm.

The reading range of the carton of pills was measured with the tag facing the reader (ie 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 and 120 cm. The reason for this increase was not immediately clear and was attributed to the undisclosed contents inside a lady's handbag!

B.4.4.4 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 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.

B.4.4.5 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.

B.4.4.6 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 x 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.

B.4.5 Eavesdropping

B.4.5.1 Introduction

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.

B.4.5.2 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 in Table B.8 here below.

Table B.8 — 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

B.4.5.3 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 100m across an open space immediately outside the Nedap building.

B.4.6 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 outside 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.

B.4.7 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.

B.5 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 – 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 – 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. However, a person intent on illicit operations may find other ways to distract the attention of an intended victim without the victim being aware that illicit reading is taking place.

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.

Although the very short operational ranges of vicinity cards and key fobs reduce the risks, reading at these ranges is still achievable. 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.

B.6 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.

Annex C

Additional Test Set ups and Results

C.1 Introduction

A Coordination Meeting between the European Commission, the CEN 225 Chairman and - Secretary and Project Team Leaders took place on 28 June 2012. During the meeting Project Team D offered to carry out some additional tests with the transmitted power of the interrogators set above the limits specified in the relevant regulatory EN Standards. It was agreed to perform these tests at both HF and UHF.

On 20 September 2012 the European Commission hosted a workshop in Brussels on RFID Privacy and Security. During the Workshop some delegates raised a concern that further work was necessary to determine the maximum range at which it was possible to read a tag. This led to a decision that PT-D should undertake additional tests to investigate the topic more deeply.

Subsequently PT-D prepared a test plan that was designed to measure the maximum range at which it was possible to read a tag from an interrogator. The power levels of the systems would be increased beyond the permitted limits in the relevant EN Standards. The test plan covered RFID systems operating both at HF and UHF. In addition it also included tests that would measure the maximum distance at which eavesdropping was possible. The draft test plan was sent to the Chairman and Secretary of CEN 225, who circulated it for comment to all members and to the Leaders of all five Project Teams. Following some revisions to the draft, it was finally approved.

It was agreed that the tests would take place at Nedap on 26 and 27 November 2012 and would be open to all members of CEN 225. In the event only three members were able to participate. These were the Leaders of Project Teams D and E and also the Chairman of ERM_TG34 in his capacity as an observer.

C.2 Scope of tests

The tests will be performed on (passive) battery less RFID tags at their two main operating frequencies. These are 13,56 MHz for HF and 865 – 868 MHz for UHF. For the purpose of the tests, RFID tags are defined as battery less transponders, which only send a response when they are within range of the energising field of an interrogator.

C.3 Documenting the results

The report shall exclude any information that is considered commercially confidential by any of the manufacturers who provide equipment to be used in the tests. The names of manufacturers who provide equipment will only be included in the report at their request.

C.4 Equipment required for additional tests

All RFID tags and interrogators used in the tests will be provided by the RFID industry and shall comply with the relevant ETSI Standards. The following specific equipment shall be provided:-

— HF equipment

  — Fixed read/write interrogator for library applications compliant with ISO 15693

  — Different interrogator's antennas with different electrical equivalent surfaces and Q factors

  — Different standard tags containing at least a unique identifier (usually 64 bits (ISO/IEC 15693))

— UHF equipment

  — Fixed RFID interrogator (EPC Class1 Gen2 or ISO 18000:—, 6C)

  — Samples of linear polarised antennas for interrogators with different gains

  — Samples of inlay tags (EPC Class1 Gen2 or ISO 18000:—, 6C)

C.5 Description of tests

C.5.1 Activation distance for HF system

C.5.1.1 General

The purpose of these tests is to establish the maximum reading range of tags when operated in typical ambient noise conditions. The tests shall be carried out in the meeting room at Nedap (the test area).

C.5.1.2 Test set up

Before the commencement of the tests the ambient noise level in the test area at the frequency of operation of the interrogators shall be measured. The level shall again be measured at the end of the tests to verify the levels have remained substantially the same.

A fixed interrogator operating in the inductive band at the specified frequency of the tags under test shall be set up in the test area and configured to operate in the continuous scroll mode. The interrogator shall be connected to a monitoring device capable of displaying tags that have been identified.

The antenna of the interrogator and the antenna of the tag shall be aligned for optimum coupling.

The tag will be fixed to a moveable part of the test bench.

The interrogator will be attached to a fixed part of the test bench.

Neither the interrogator nor the tags shall be rotated in any way from their optimum alignment during the tests.

Figure C.1 shows the test set-up for range measurement:

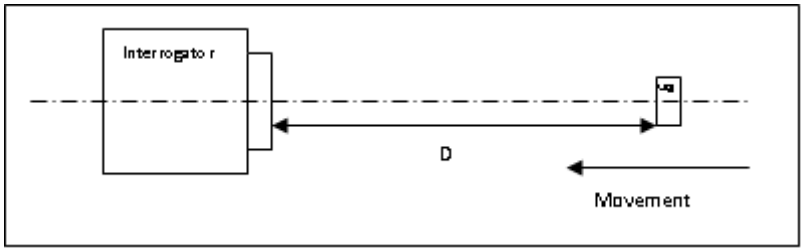

Figure C.1 — Test setup for Operated Range Test

C.5.1.3 Test Procedure

The interrogator shall be configured to operate at its maximum permitted power level at the correct operating frequency for the tag and in accordance with local radio frequency regulations. The sensitivity of the interrogator, its modulation index and data rate shall be recorded. Tag shall be mounted on a non-magnetic material (eg. foam, paper, plastic…)

1) Initially the tag under test shall be positioned beyond its maximum reading range so that the interrogator is not able to decode any response from the tag.

2) The tag shall be moved closer to the interrogator by the following increments:

— 0,5 cm step if D < 10 cm.

— 1 cm step if 10 cm ≤ D ≤ 50 cm.

— 2 cm step if D > 50 cm.

3) The Inventory command or Read command (as applicable) shall be sent by the interrogator for each position of the tag and the existence of a communication link shall be verified.

4) If the communication link does not exist, step 2 shall be repeated.

5) If the communication link exists, the read command shall be repeated 3 times without moving the tag.

6) If any one of the read commands fails, then the step 2 shall be repeated.

7) If the communication link exists for each of the 3 read commends, then the distance D shall be noted in the report as the “IDENTIFICATION_RANGE” or “READ_RANGE” (as applicable).

8) Steps 1-7 shall be repeated for different values of interrogator's conducted powers. These values shall be recorded in the test report. *What is the purpose of changing the transmit power? Surely we are only interested in maximum reading range?*

9) Steps 1-8 shall be repeated for different interrogator's antenna sizes (values of electrical antenna size and Q factors shall be recorded) *What is the purpose of this?*

10) Steps 1-9 shall be repeated for each tag under test.

These tests may require field strengths that exceed the recommended human exposure limits to EMF and appropriate precautions should be taken.

C.5.2 Activation distance for UHF system

C.5.2.1 Introduction

The purpose of these tests is to establish the reading range of tags when operated in typical ambient noise conditions. The tests shall be carried out in the meeting room at Nedap (the test area). The tag under test shall be fixed to an electromagnetic transparent material (eg. foam, paper, plastic…)

C.5.2.2 Test set up

A fixed interrogator operating in the UHF band at the specified frequency of the tags under test shall be set up in the test area and configured to operate in the continuous scroll mode. The interrogator shall be connected to a monitoring device capable of displaying tags that have been identified.

The antenna of the interrogator and the antenna of the tag shall be aligned for optimum coupling. The antenna of the interrogator shall be linearly polarised.

The tag will be attached to a mobile part of the test bench.

The interrogator will be set up on a fixed part of the test bench.

Neither the interrogator nor the tags shall be rotated in any way from their optimum alignment during the course of the tests..

Figure C.1 shows the test set-up for range measurement.

C.5.2.3 Procedure

The interrogator shall be configured to operate at its maximum permitted power level in one of the designated high power channels in accordance with the local radio frequency regulations. The sensitivity of the interrogator, the modulation index, the data coding format and the data rate shall be recorded.

1) Initially the tag under test shall be positioned beyond its maximum reading range so that the interrogator is not able to decode any response from the tag

2) The tag shall be moved closer to the interrogator by the following increments:

— 0.5 cm step if D < 10 cm;

— 1 cm step if 10 cm ≤ D ≤ 50 cm;

— 2 cm step if D > 50 cm.

3) The Inventory command or Read command (as applicable) shall be sent by the interrogator for each position of the tag and the existence of a communication link shall be verified.

4) If the communication link does not exist, the step 2 shall be repeated.

5) If the communication link exists, the read command shall be repeated 3 times without moving the tag.

6) If one out of the 3 read commands fails, then the step 2 shall be repeated.

7) If the communication link exists for all 3 read commands then the distance D shall be noted in the report as the “IDENTIFICATION_RANGE” or “READ_RANGE” (as applicable).

8) Steps 1-7 shall be repeated for different values of E.R.P for the interrogator. These values shall be recorded in the test report. *See my comment in previous section*

9) Steps 1-8 shall be repeated for each tag under test.

These tests may require field strengths that exceed the recommended human exposure limits to EMF and appropriate precautions should be taken.

C.5.3 Eavesdropping tests for HF system

C.5.3.1 Introduction

The purpose of these tests is to establish the range at which it is possible for a receiver to read the response from a tag that is activated by a HF RFID system. Measurements will be performed with loop antennas which will eavesdrop only magnetic field. Eavesdropping HF RFID communications using electric field in the far field region is out of the scope of these tests.

C.5.3.2 Test set up

A fixed interrogator operating at HF (13,56 MHz) shall be set up in the test area and configured to operate in continuous scroll mode. The interrogator shall be connected to a monitoring device capable of displaying tags that have been identified. A spectrum analyser (or measurement receiver) tuned to the same operating

frequency as the interrogator shall be connected to a monitoring device. The sensitivity of the receiver shall be at least that found in a typical interrogator.

The antenna of the interrogator and the antenna of the tag shall be aligned for optimum coupling.

The tag will be positioned on a fixed part of the test bench.

The interrogator will be positioned on a fixed part of the test bench.

The receiver will be fixed on a mobile part of the test bench.

Neither the interrogator, nor the receiver nor the tags shall be rotated in any way from their optimum alignment during the course of the tests.

Figure C.2 here below shows the test set-up for the eavesdropping measurement:

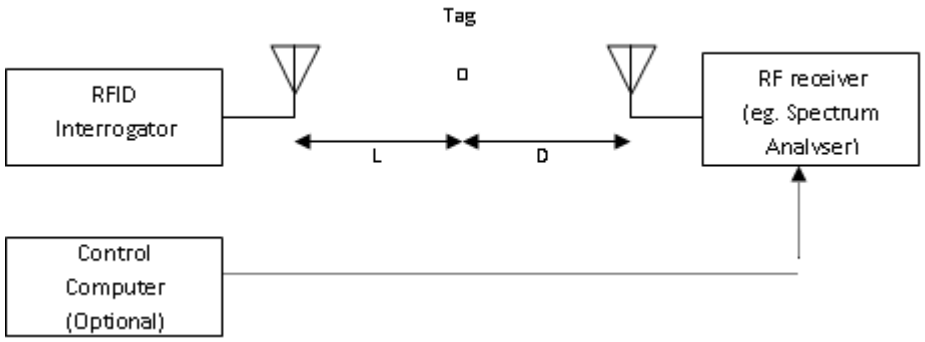

Figure C.2 — Test set-up for eavesdropping measurement

C.5.3.3 Procedure

The interrogator shall be set up to operate at its maximum power level in accordance with Figure C.2 and in accordance with local radio frequency regulations. The modulation index and data rate shall be recorded. A tag shall be fixed to a non magnetic material (eg. foam, paper, plastic…)

1) A tag shall be placed in front of the RFID interrogator. The distance L between the tag and the antenna of the interrogator's shall be adjusted so that the signal from the tag is at a maximum.

2) The monitoring receiver will be positioned at least D=1 m from the tag and a check made to verify that it is receiving the response from the tag.

3) The receiver shall be moved away from the tag to a point at which it is just able to detect the response from the tag.

4) The maximum distance D at which the receiver is just able to detect the signal modulated by the tag shall be recorded*. Note that there is a material difference between detecting the presence of the response from the tag and being able to read the data*

5) The sensitivity of the monitoring receiver shall be recorded.

6) Steps 2-5 shall be repeated for different receiver antenna sizes (values of electrical antenna size and Q factors shall be recorded). *Which antennas will be changed? The only one of relevance is the one connected to the spectrum analyser. Incidentally I am not sure how useful this is. If the gains are known the difference in range can be calculated*

7) Steps 1-6 shall be repeated for each tag under test.

C.5.4 Eavesdropping tests for UHF system

C.5.4.1 Introduction

The purpose of these tests is to establish the range at which it is possible for a receiver to read the response from a tag that is activated by a UHF RFID system.

C.5.4.2 Test set up

A fixed interrogator operating at UHF (865 - 868 MHz) shall be set up in the test area and configured to operate in continuous scroll mode. The interrogator shall be connected to a monitoring device capable of displaying tags that have been identified. A spectrum analyser (or measurement receiver) tuned to the same operating frequency as the interrogator shall be connected to a monitoring device. The sensitivity of the receiver shall be at least that found in a typical interrogator.

The antenna of the interrogator and the antenna of the tag shall be aligned for optimum coupling. The antennas of both the Interrogator and receiver shall be linearly polarised.

The tag will be positioned on a fixed part of the test bench.

The interrogator will be positioned on a fixed part of the test bench.

The receiver will be positioned on a mobile part of the test bench.

Neither the interrogator, nor the receiver nor the tags shall be rotated from their optimum alignment during the course of the tests.

Figure C.2 here above shows the test set-up arrangements for the eavesdropping measurement.

C.5.4.3 Procedure

The interrogator shall be set up to operate at its maximum power level in accordance with Figure C.2 and in accordance with radio frequency local regulations. The modulation index, data coding and data rate shall be recorded. Tag shall be fixed to an electromagnetic transparent material (eg. foam, paper, plastic…).

1) A tag shall be placed in front of the RFID interrogator. The distance L between the tag and the antenna of the interrogator's shall be adjusted so that the signal from the tag is at a maximum.

2) The monitoring receiver will be positioned at least D=1 m from the tag and a check made to verify that it is receiving the response from the tag.

3) The receiver shall be moved away from the tag to a point at which it is just able to detect the response from the tag. *Note that there is a material difference between detecting the presence of the response from the tag and being able to read the data*

4) The maximum distance D at which the receiver is just able to detect the signal modulated by the tag shall be recorded. *Note that it may be necessary to use a filter in order to detect the signal from the tag. See* Clause 10 *of* EN 302 208 *v1.4.1*

5) The sensitivity of the monitoring receiver shall be recorded.

6) Steps 2-5 shall be repeated for different receiver antenna gains. Receiver antenna gains shall be recorded in the test report. *See comment in previous clause*

7) Steps 1-6 shall be repeated for each tag under test.

C.6 Test results

C.6.1 Equipment utilised during the tests

The following equipment was used in the course of carrying out the tests:

High Frequency (13,56 MHz**)**

1) Nedap Interrogator DVD MK 1 (see www.nedap.com)
2) Loop antenna (40 x 150 cm) for library use – PG50, single loop, see Figure C.3
3) General purpose HF vicinity cards – NXP SLI (ISO 15693)

UHF (865 – 868 MHz)

4) Nedap !D Top interrogator see Figure C.12
5) !D Top antenna with linear polarisation, see Figures C.13 and C.14
6) Two different designs of retail label tag (UPM Belt and AD232)

Test equipment

7) Rhode and Schwartz Measurement receiver Type EB200
8) Lindgren loop antenna Type ETS 6512
9) Rhode and Schwartz magnetic loop active antenna HE200
10) Rhode and Schwartz spectrum analyzer Type FSV
11) Diamond Antenna SX-200 SWR power meter
12) Nedap !D Top antenna (see Figure C.12)

C.6.2 Description of Tests

C.6.2.1 Introduction

The following subclauses will describe the ambient noise measurement, the tests on the activation distance of the tags on HF and UHF at power~~s~~ levels above the regulatory limits. Also the results are displayed in ~~a~~ corresponding graphs.

C.6.2.2 Measurement of ambient noise

The measurement of ambient noise at HF was made using a spectrum analyzer connected to a loop antenna. In accordance with CEPT Recommendation 74-01, the spectrum analyzer was set to measure the average level in a reference bandwidth of 100 kHz. At a centre frequency of 13,56 MHz this gave an adjusted level of 42 dBµV/m.

The measurement of the ambient noise level at UHF was made using the !D Top antenna connected to a spectrum analyzer. The spectrum analyzer was set to "max hold" and the reading was recorded using a resolution bandwidth of 100 kHz. This gave an adjusted figure of - 92 dBm/100 kHz around a centre frequency of 866 MHz.

C.6.2.3 HF Measurements

C.6.2.4 Introduction

C.6.2.4.1 General

The purpose of these tests is to establish the maximum activation range of HF-tags with powers beyond the regulatory limit according to EN 300 330, when operated in a typical ambient noise environment. Also the eavesdropping range has been measured.

C.6.2.4.2 Interrogator

The tests were performed using a standard interrogator system for libraries operating at 13,56 MHz that was provided by Nedap. This had a large loop antenna that ensured that energising magnetic field filled a volume that extended about 1,5 m on either side of the structure, see Figure C.3.

Figure C.3 — Loop antenna for the library system

C.6.2.4.3 Tags

Five different tags were used with dimension 75 by 45 mm see Figures C.4 to C.8

Figure C.4 — Library tag number 1

Figure C.5 — Library Tag number 2

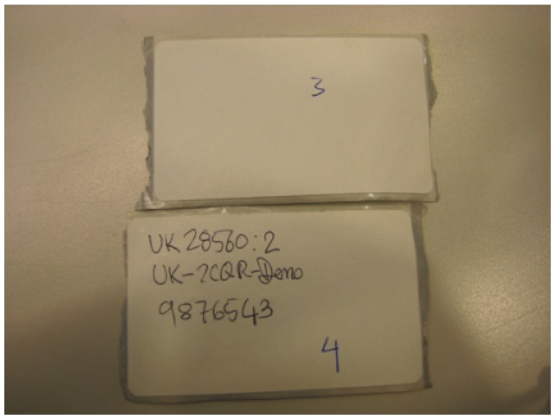

Figure C.6 — Library tag number 3 and 4

Figure C.7 — Library tag number 5

Figure C.8 — Label shape dimension 75 by 45 mm

C.6.2.4.4 Maximum Activation Range

The tags in turn were used to determine the maximum range at which it was possible to activate a tag see Figure C.9. Indication of a valid activation was given by an audible signal from the interrogator.

Figure C.9 — Library system with library tag and loop antenna

Measurements were first made with the interrogator set to its maximum possible output of 63,7 dBµA/m @ 10m. The limit at 13,56 MHz according to EN 300 330 is 60 dBµA/m @ 10m, so the field strength of the library system with the PG50 antenna was slightly over the regulatory limit. The tests were then repeated with a reduced output of 53,9 dBµA/m @ 10m.

The maximum activation ranges of the tags from the loop antenna are provided in Table C.1.

Table C.1 — Activation ranges of tags at HF

Tag number	Activation range in cm	
	Field strength 53,9 dBµA/m@10m	Field strength 63,7 dBµA/m@10m
1	32	60
2	70	108
3	78	120
4	36	70
5	40	81

The maximum range at which a tag 3 could be activated was in the order of 1,2 m.

NOTE 53,9 dBµA/m = 496 µA/m, 63,7 dBµA/m = 1532 µA/m. EN 300 330 limit is 1000 µA/m @ 10 m.

Figure C.10 shows the activation range as function of the transmitted field strength at 10 m distance for tag number 3.

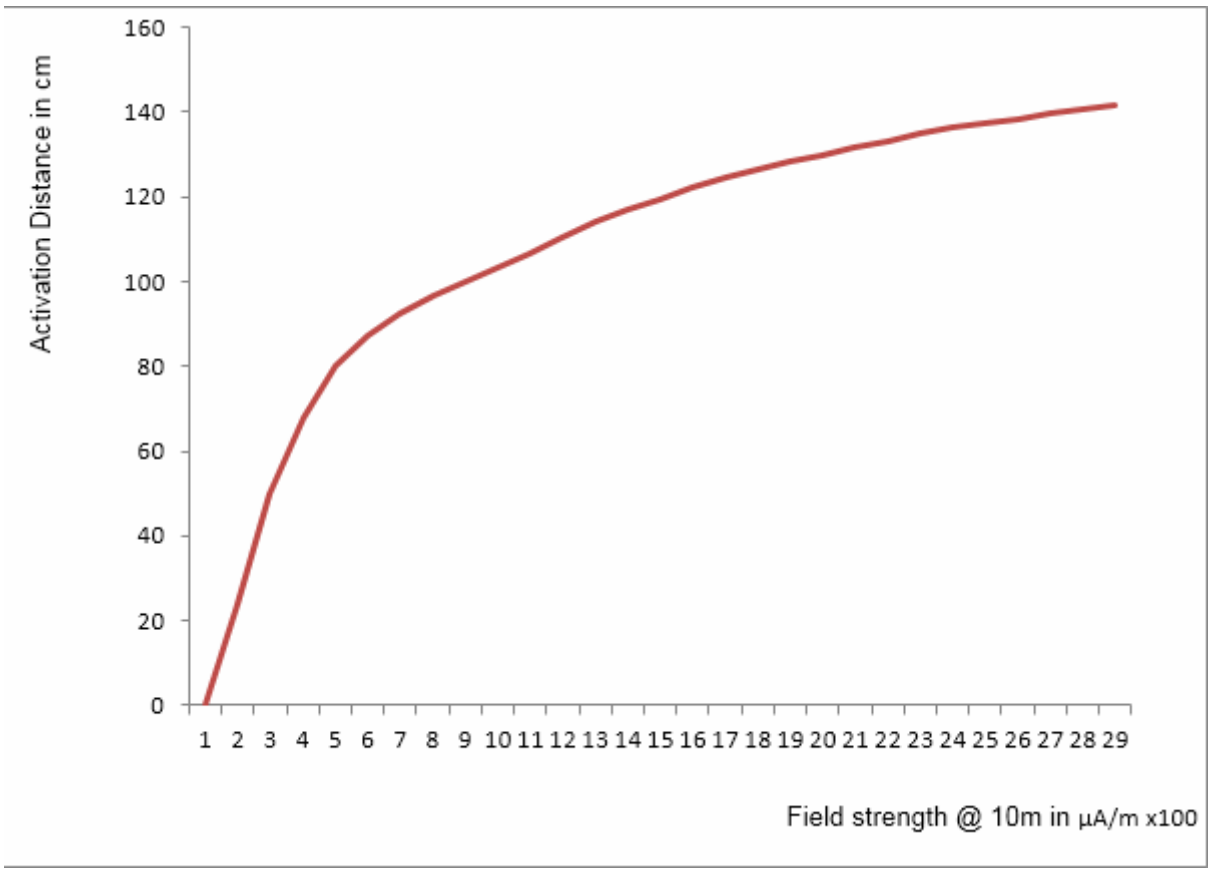

Figure C.10 — HF Activation distance as function of the field strength @ 10 m distance

C.6.2.4.5 Maximum Eavesdropping Range

In order to measure the range at which it was possible to eavesdrop on an HF tag, an active loop antenna was connected to the spectrum analyzer. The spectrum analyzer was set up in the time domain so that it was possible to distinguish between the modulated transmissions from the interrogator and the response from the tag see Figure C.11. It was considered that an appropriate level at which it would be just possible to decode a tag signal would be 3 dBm above ambient noise level.

Figure C.11 — Trace of tag response using an active antenna

Three library tags were selected for the test (see tags from Figures C.5 and C.6). Each one was positioned in turn at a distance of about 30 cm from the loop antenna of the library system. The emission from the tag was observed on the spectrum analyzer. The active loop antenna was rotated to give maximum response for the signal from the tag and the range gradually increased. When the signal from the tag had dropped to a level of 3 dB above ambient, the range was recorded. The same procedure was repeated for the other two library tags. The results from the measurements are shown in Table C.2. For the measurements, the field strength of the interrogator was set to 63,7 dBµA/m @ 10m.

Table C.2 — Maximum ranges for eavesdropping at HF

Tag number	Eavesdropping range in cm
2	209 cm
3	320 cm
4	295 cm

Under the measurements conditions (receiver sensitivity, floor noise, tag backscattered signal strength, …), the maximum distance recorded at which it was possible to eavesdrop on a tag is 3,2 m.

C.6.2.5 Measurements at UHF

C.6.2.6 Introduction

C.6.2.6.1 General

The purpose of these tests is to establish the maximum activation range of UHF-tags with power levels beyond the regulatory limit according to EN 302 208, when operated in a typical ambient noise environment. Also the eavesdrop range has been measured.

C.6.2.6.2 Interrogator

Measurements were initially made with the interrogator set to give a conducted output of 32 dBm connected to an antenna with a net gain of 11 dBi. Taking into account the correction of 2 dB from e.i.r.p. to e.r.p., this gave an output level of 41 dBm e.r.p. equivalent to 12,6 W e.r.p. which is significantly greater than the regulatory limit of 33 dBm e.r.p (=2 W e.r.p.) according to EN 302 208. (see Figure C.12 to Figure C.14).

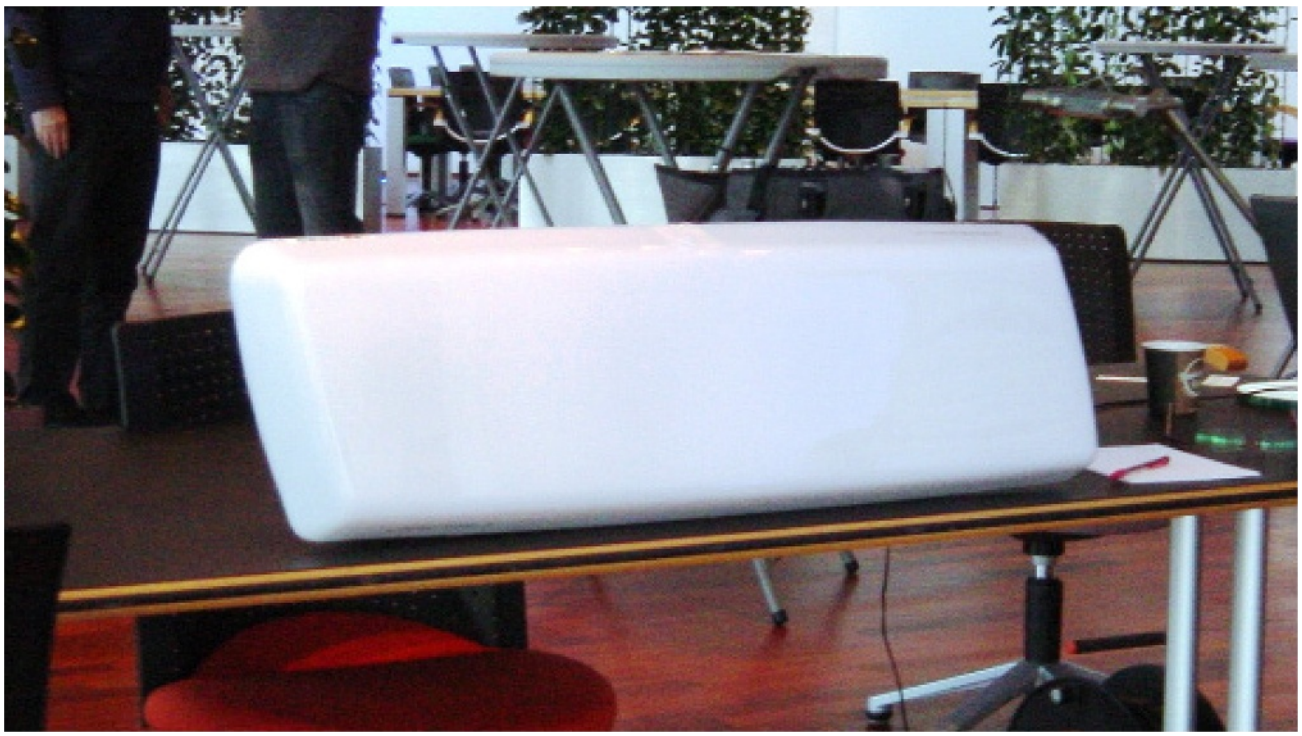

Figure C.12 — Front view of !D Top interrogator with integrated antenna

Figure C.13 — Integrated antenna dimensions of the !D Top interrogator

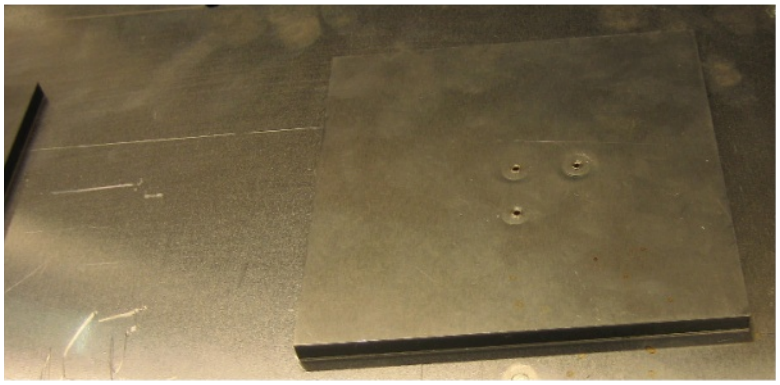

Figure C.14 — Antenna dimensions of the !D Top interrogator 112 by 122 mm

C.6.2.6.3 Tags

Two types of tags A and B as shown in Figure C.15 were utilised for the tests. Tags of Type A, with number 1 to 3, were selected because these were known to be particular sensitive. Tags of Type B numbered 11 and 12 were typical of those found in general use within the retail sector.

Figure C.15 — The two types of retail tag (Type A at top and Type B at bottom)

C.6.2.6.4 Maximum activation range

Following the procedure specified in the test plan, the maximum range was measured at two output levels. The tests were conducted with an initial output power of 41 dBm equivalent to 12,6 W. The tests were then repeated with output level reduced to 33 dBm e.r.p equivalent to 2 W e.r.p. see also Figure C.16.

Figure C.16 — Photo showing the activation range at max power

There was a significant difference between the maximum activation ranges of the two types of tag. Tags of type A, which were numbered 1 to 3, had a much higher activation rage were selected because they were known to be particularly sensitive. Tags of type B numbered 11 and 12, were typical of those found in general use within the retail industry.

The results of the measurements are presented in Table C.3.

Table C.3 — Activation ranges measured at UHF

Tag number	Activation Range in m @ 2 W e.r.p.	Activation Range in m @ 12,6 W e.r.p.
1	9,8	19,6
2	9,9	21,0
3	9,9	21,2
11	4,1	12,0
12	4,0	11,9

NOTE The allowed power according to the CEPT Recommendation 70-03 and the EN 302 208 is 33 dBm that is equivalent to 2 W e.r.p.

Figure C.17 shows the activation range as function of the transmitter power in W e.r.p. for UHF tag number 3.

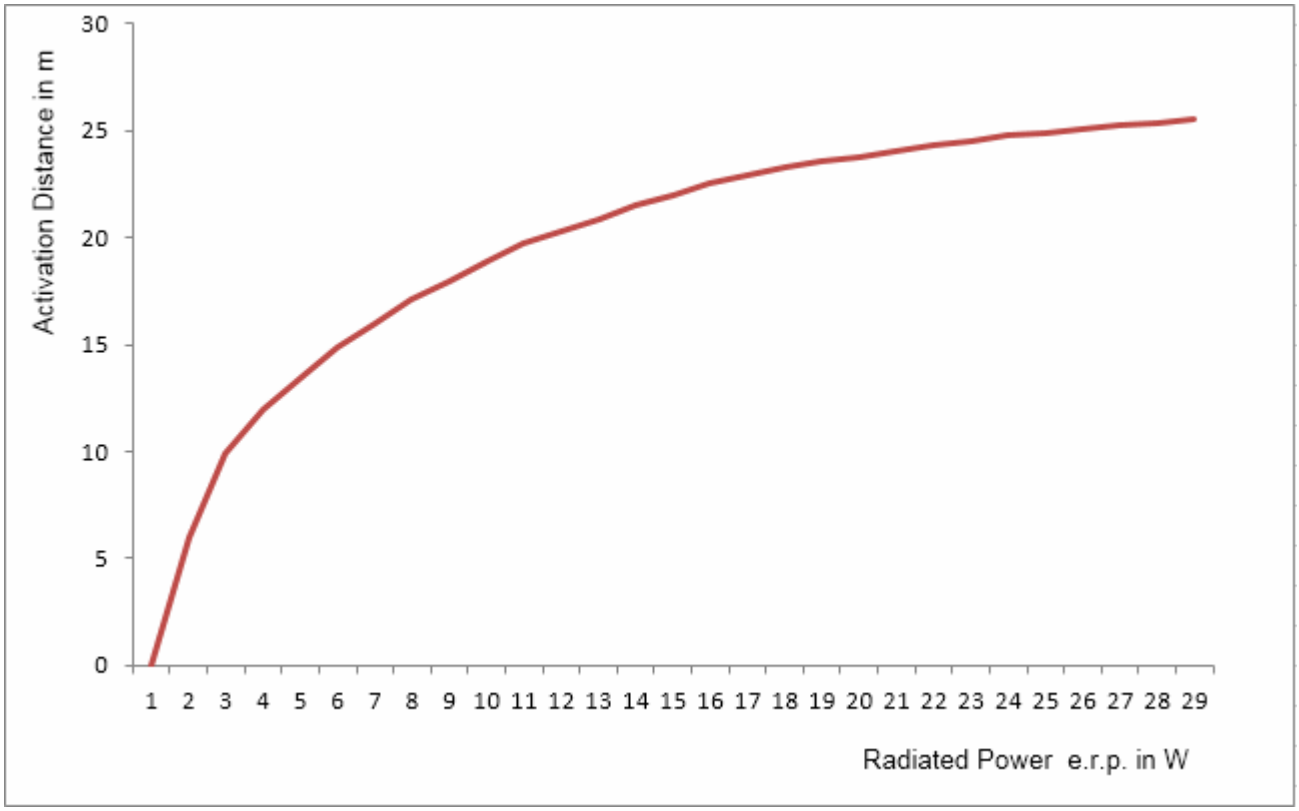

Figure C.17 — UHF Activation distance as function of the transmitter power in W e.r.p.

C.6.2.6.5 Eavesdropping

Tests were carried out to determine the maximum range at which it was possible to read the data in a tag. The tests were limited to type A tags only since they would clearly produce the highest figure. The measurements were performed as follows.

The tags were mounted in turn on the support that was positioned outside the building. Although this did not equate to free-space conditions, it nevertheless gave an unobstructed view over a distance of about 80 m. The !D Top interrogator was positioned with its antenna about 1,5 m from the support to ensure that the tag was fully energised see Figure C.18. The interrogator was configured to ensure that the tag under test sent a continuous stream of messages.

Figure C.18 — Set-up of equipment for eavesdropping test at UHF

The messages from the tag were measured using a battery powered receiver connected to the !DTop antenna. The receiver was tuned to receive the emissions from the tag but to reject the transmit signals from the interrogator.

Before starting the test there was a discussion on the level to be used to assess whether a signal from the tag could be decoded. Assuming a C/I of say 10 dB and an average ambient noise level of around -100 dBm, this equates to a receive signal level from the tag of about - 90 dBm.

Allowing for the antenna gain and set-up of the receiver the -90 dBm was equivalent to a reading on the display of the Rhode & Schwarz EB 200 connected to the !D Top antenna of 17 dBµV see Figure C.19 and C.20.

Figure C.19 — Eavesdropping test at UHF

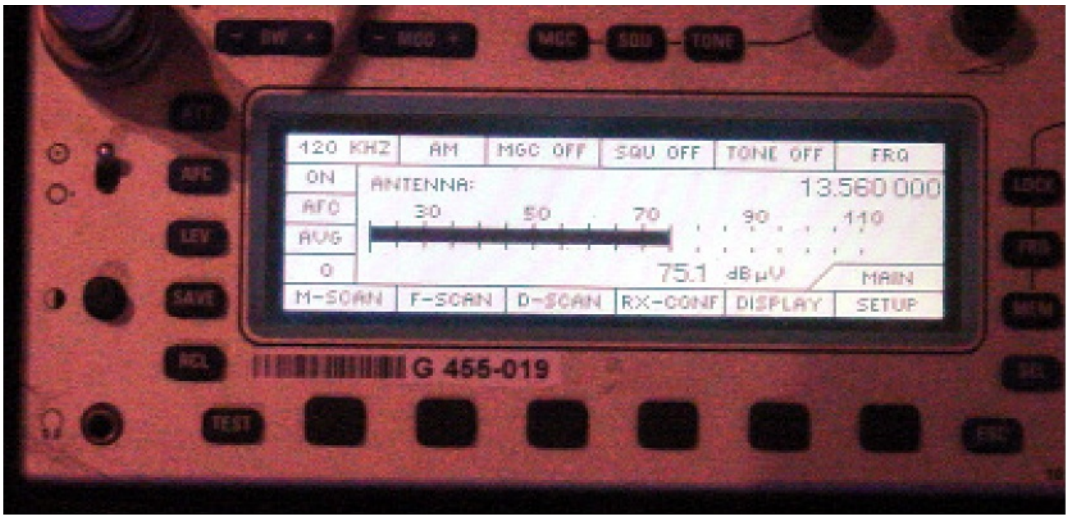

Figure C.20 — Display on portable receiver

With tag 1 mounted on the support, the distance of the receiver from the tag was slowly increased according to procedure while ensuring that the level of the received signal from the tag remained above the threshold. During this process it was necessary periodically to verify that the signal being received came from tag 1 rather than from other tags that were intermittently in operation in the Nedap premises.

At a distance of 80 m the reading on the receiver had fallen to 12 – 14 dBµV, which the Nedap engineer said was at about the limit of what was detectable. The tests were repeated for tags 2 and 3. These gave readings at a range of 80 m of 15 – 16 dBµV and 14 - 16 dBµV respectively. Based on these results it was concluded

that the maximum range at which it would be possible to eavesdrop on a tag in low levels of ambient noise was 80 m (under the measurement conditions: receiver sensitivity, floor noise, tag backscattered signal strength, ...).

C.6.2.7 Discussion

1) The tests at UHF were performed at relatively low levels of ambient noise. This will not always be the case. Higher noise levels will lead to a reduction in the maximum activation range that is achievable. For example it is anticipated that the imminent deployment of LTE (=Long Term Evolution, 4G) below 860 MHz is likely to introduce significant levels of wide band noise into the SRD band. Practical tests have demonstrated that this could potentially reduce the maximum activation range of RFID systems.

2) During the tests it was noted that there were other RFID systems that were also in operation at the Nedap premises. While performing the eavesdropping tests at UHF it was very difficult to know which tags were being received. The only way that this could be resolved with any certainty was for the tag under test to be silenced. In a real eavesdropping scenario this would not be an option. As a result for many eavesdropping activities performed over no more than a very short distance, identification of the source of the tag would be difficult.

3) It was very apparent to all present at the tests that the level of technical skill and commitment necessary to read a tag illicitly is quite considerable.

4) The tests on the library system operating at HF were performed with the equipment positioned in the centre of the test area. However situations may arise where the system is installed close to magnetically conductive material. This can result in the magnetic fields generated by the system travelling along the conductive material. In such circumstances it may be possible to read a tag at greater distances than those achieved in the tests.

5) The additional measurements described in these tests should enable the reader of this report to estimate the maximum range that can be achieved at different levels of transmitted power.

C.6.2.8 Conclusion

The following conclusions may be drawn from the tests.

1) The results of the tests show that the activation range of a RFID system at a frequency of 13,56 MHz and a normal gate antenna in a library environment is reaching a limit of approximately 1,6 m when the field strength is increased to levels far beyond the regulatory limit. Under the measurements conditions (receiver sensitivity, floor noise, tag backscattered signal strength, …), the maximum distance recorded at which it was possible to eavesdrop on a tag is 3,2 m

2) The results of the tests show that the activation range of a RFID system at a frequency of 865 – 868 MHz and a normal antenna applied in the retail environment is reaching a limit of approximately 25-27 m when the power is increased to levels far beyond the regulatory limit. Under the measurements conditions (receiver sensitivity, floor noise, tag backscattered signal strength, …), the eavesdropping maximum range is 80 m.

3) Undertaking the tests in the test plan demonstrated to the test team that obtaining useful personal data by means of illicit reading or eavesdropping is more difficult than commonly understood.

4) These measurements finally will help RFID operators while undertaking a PIA process to assess the likelihood of an illicit activation and/or eavesdropping and assess the required skills and equipment to make an attack possible.

Bibliography

[1] ISO/IEC 18000-1, *Information technology — Radio frequency identification for item management — Part 1: Reference architecture and definition of parameters to be standardized*

[2] ISO/IEC 18000-2, *Information technology — Radio frequency identification for item management — Part 2: Parameters for air interface communications below 135 kHz*

[3] ISO/IEC 18000-3, *Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13,56 MHz*

[4] ISO/IEC 18000-4, *Information technology — Radio frequency identification for item management — Part 4: Parameters for air interface communications at 2,45 GHz*

[5] ISO/IEC 18000-6, *Information technology — Radio frequency identification for item management — Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General*

[6] ISO/IEC 18000-61, *Information technology — Radio frequency identification for item management — Part 61: Parameters for air interface communications at 860 MHz to 960 MHz Type A*

[7] ISO/IEC 18000-62, *Information technology — Radio frequency identification for item management — Part 62: Parameters for air interface communications at 860 MHz to 960 MHz Type B*

[8] ISO/IEC 18000-63, *Information technology — Radio frequency identification for item management — Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C*

[9] ISO/IEC 18000-64, *Information technology — Radio frequency identification for item management — Part 64: Parameters for air interface communications at 860 MHz to 960 MHz Type D*

[10] ISO/IEC 18000-7, *Information technology — Radio frequency identification for item management — Part 7: Parameters for active air interface communications at 433 MHz*

[11] ISO/IEC 18046-1, *Information technology — Radio frequency identification device performance test methods — Part 1: Test methods for system performance*

[12] RIEBACK M.R., GAYDADJIEV G.N., CRISPO B., HOFMAN R.F.H., TANENBAUM A.S. "A Platform for RFID Security and Privacy Administration" 20th USENIX/SAGE Large Installation System Administration conference (LISA 2006), Washington DC, December 2006.

[13] ETSI/TR 101543v1.1.1 (2011-04) Electromagnetic compatibility and radio spectrum matters (ERM); RFID Evaluation tests undertaken in support of Phase 1

[14] M.R. Rieback, Patrick N.D. Simpson, B. Crispo, A.S. Tanenbaum. "RFID Malware: Design Principles and Examples" Pervasive and Mobile Computing (PMC) Journal, vol. 2(4): 405-426, Elsevier, 2006.

[15] RIEBACK M.R., CRISPO B., TANENBAUM A.S. "RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management." Proc. 10th Australasian Conference on Information Security and Privacy. (ACISP 2005), Brisbane, Australia, July 2005

[16] RIEBACK M.R., CRISPO B., TANENBAUM A.S. "Uniting Legislation with RFID Privacy-Enhancing Technologies." Proc. 3rd Conference on Security and Protection of Information. (SPI 2005), Brno, Czech Republic, May 2005.

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™