Open Smart Card Infrastructure for Europe

v2

Volume 6: **Contactless Technology**

Part 2: **White paper on Security and Threat Evaluation relating to Contactless Cards**

Authors: **eESC TB6 Contactless Smart Cards**

NOTICE

This eESC Common Specification document supersedes all previous versions.

Neither eEurope Smart Cards nor any of its participants accept any responsibility whatsoever for damages or liability, direct or consequential, which may result from use of this document.

Latest version of OSCIE and any additions are available via www.eeurope-smartcards.org and www.eurosmart.com. For more information contact info@eeurope-smartcards.org.

Contents

Page

.

Foreword

This document was developed as part of the eEurope Smart Card Charter, within the Trailblazer 6 Contactless Technology working group. This document is also the result of a joint work undertaken by the members of the 'SINCE' project in Work Package 1, item 2: security. The contributors to this document are Gemplus, INSIDE Technologies, SchlumbergerSema, Spirtech, STMicroelectronics and Telecom Italia Lab.

Introduction

The primary objective of eEurope TB6 and the SINCE project is to promote, harmonise and stimulate the widespread uptake of contactless technology. The SINCE project fits within the framework of the eEurope initiative launched by the European Commission in December 1999, the Smart Cards Charter original objectives : eCommerce development; distribution of interoperable multi-applications cards, promotion of use of contactless cards and development of the European smart card industry and the main objectives of the Cross Program Action 5 (CPA5) : increase smart card deployment, both on items a) for deploying innovative applications and services to foster the build up of a critical mass of users for smart card applications and c) for advancing smart card technologies. SINCE will contribute to achieve a leading position for European e- and m-commerce applications and finally, SINCE is one of the main contributors to bring" Information Society closer to the European Citizen, more informative and helpful".

.

1 Scope

The security of contact smartcard based products and systems has been well documented and has been the focus of some very detailed work and analysis in the past. Contact smartcards have consequently reached such a maturity that they are considered as privileged tamper resistant devices to store sensitive data and to perform sensitive operations on these data. On the other hand, contactless technology is still in its early stages. As such, **its security needs to be analysed in the same detail if it is to be able to compete in equal terms with contact technology.** The goal of this document is to start the process and encourage the sharing of knowledge on this issue. The aim is to stimulate the industrial community, the operators and the laboratories involved in evaluations into switching some of their efforts, in the field of security, into contactless technology.

2 Terms and definitions

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

AFI	Application Family Identifier
APDU	Application Protocol Data Unit
ASIC	Application Specific Integrated Circuit
ASK	Amplitude Shift Key
CCD	Contactless Coupling Device
CICC	Contactless Integrated Circuit(s) Cards
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DPA	Differential Power Analysis
EOF	End Of Frame
EEPROM	Electrically Erasable Programmable Read Only Memory
FSK	Frequency Shift Keying
IEC	International Electrotechnical Commission
IFD	InterFace Device
ISO	International Standardization Organization
ITU	International Telecommunications Union
MCU	MicroController Unit
MMU	Memory Management Unit
NRZ	Non Return to Zero
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit(s) Cards
PP	Protection Profile
PSK	Phase Shift Keying
RAM	Random Access Memory
RF	Radio Frequency
RFID	Radio Frequency IDentification
ROM	Read Only Memory
SOF	Start Of Frame
SPA	Simple Power Analysis
UID	Unique ID
VCD	Vicinity Coupling Device
VICC	Vicinity Integrated Circuit(s) Cards

3 Contactless Technology Description

NOTE: This section of the document provides an overview of Contactless Technology and is partly reproduced in all CSv2 Volume 6 reports and SINCE deliverables for convenience.

3.1 Introduction

The contactless RF technology has been available for almost as long as the smart card technology, in fact as early as 1986 in the United States RFID fish tags were produced for tracking salmons [1]. In 1991, the RATP and Innovatron decided to work together to produce the core of a contactless ticketing system for the Paris underground, bus and regional railway system and in 1993 a range of memory products operating at 6,78 MHz and later at 13,56 MHz were developed and deployed on the RATP network [2].

The semiconductor manufacturers began to design chips that were able to transmit and to receive data over the air, but also to receive enough power to drive the electronic circuitry on the card. This was first achieved with RF tags and memory devices. The need for more secure and more versatile products has driven contactless technology from a memory based product to a microprocessor based product which is able to give the users more value added services.

The figure below shows the contactless chip evolution.

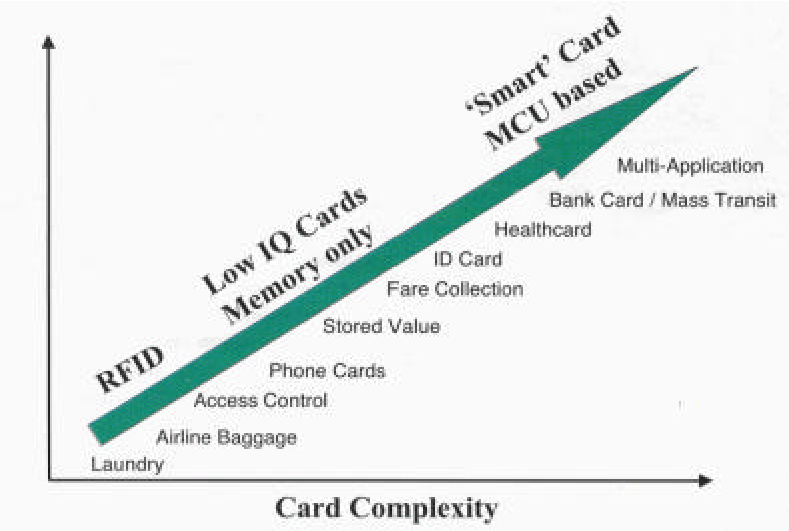


Figure 1 - Contactless chip evolution [1]

The Contactless Card is an integrated circuit card that enables energy to flow between the card and the interfacing device without direct physical contact. Instead, induction or high-frequency transmission techniques are used through a radio frequency (RF) interface.

3.2 Power Supply

Contactless Cards are generally powered by an RF field. Contactless cards contain an electronic element that is called transponder. A transponder consist of an inductive antenna and a microchip connected to the ends of the antenna. For better protection of the microchip, it is usually packaged in a module and the antenna is then interconnected to the module. The transponder is embedded in the contactless card plastic support as shown in Figure 2.

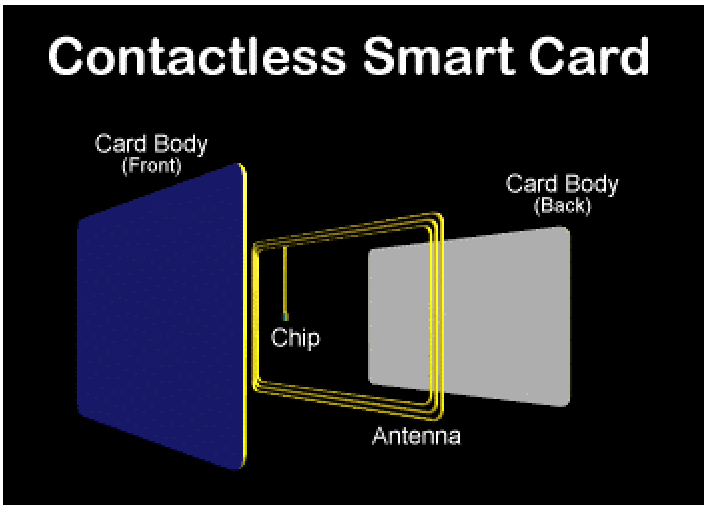


Figure 2 - Contactless card structure [3]

In this case an inductive coupling will transmit both power and data through the air or a non metallic surface from the IFD (InterFace Device) to the contactless card. The RF energy received by the contactless card antenna embedded in the card is converted in a DC voltage in order to power the card's internal circuits. Power conversion is done with a full bridge rectifier (see Figure 3).

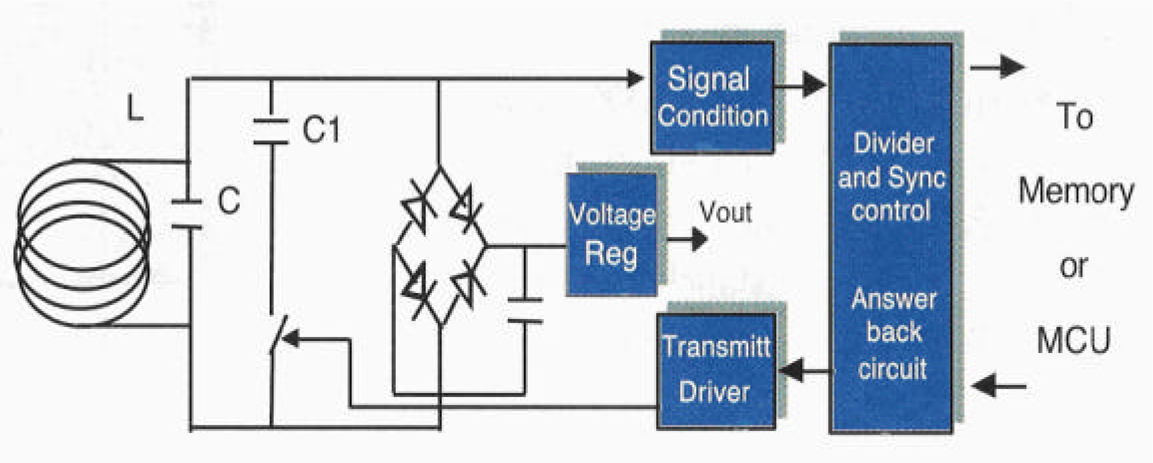


Figure 3 - Typical RF contactless receiver [1]

Another way of looking at the power coupling is to view the card and the card reader antenna coils as component of an RF transformer. The transformer's primary coil is in the card reader; the secondary coil is in the card. The space between the coils is the transformer's air core. The card antenna may be parallel tuned to increase the coupling efficiency.

The diagram (Figure 4) illustrates the RF energy coupling between a card and a reader. The card receives the signal, decodes it, and responds back to the reader.

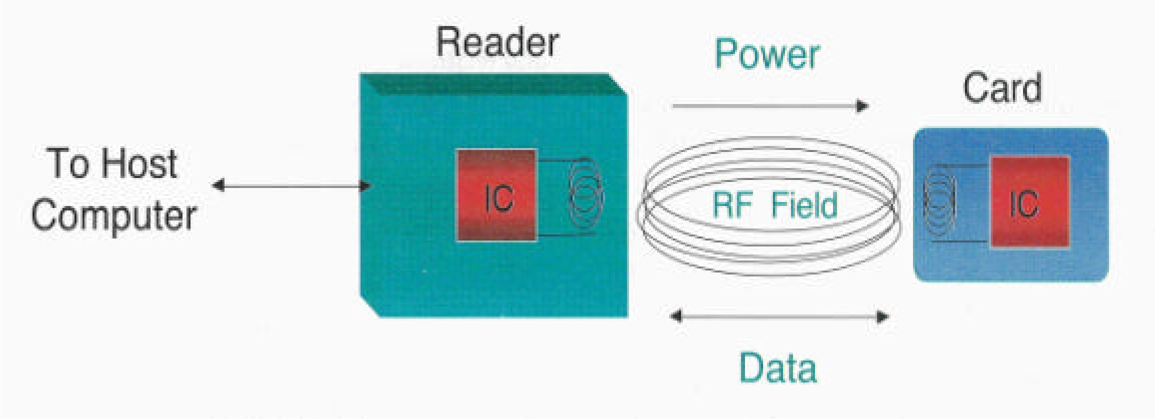


Figure 4 - Contactless card in an RF field [1]

3.3 Communication

Contactless cards use an RF interface between the IFD and the card in order to communicate with the IFD. The communication may be inductive or capacitive, it depends on the type of Contactless Card.

Inductive Coupling

Inductive coupling involves the use of two coils of wire - one acts as a primary coil and one acts as a secondary coil. An alternating current passes through a primary coil that creates an alternating magnetic field, which induces a flow of current in the secondary coil when they are in close proximity. Modulating the current at two different frequencies as it passes through the primary coil allows data to be transmitted to the secondary coil. When the card receives the current, it demodulates the signal and retrieves the data at the same time as it uses the transmitted power to activate its circuitry. Therefore, the advantage of this process is that it is able to transfer both information and power to a smart card.

Inductive coupling contactless cards can basically be divided into two groups ruled by the operating frequency they use to exchange data. The older of the two basic types operates at 125 kHz. These cards are mainly in use for access control to buildings and industrial applications. The inductance of the coils needs to be in the mH range, therefore a typical antenna in card format consists of 300 turns of thin insulated copper wire. The second type operates at 13,56 MHz. These cards are used where transaction speed is critical. The inductance of these antennae is in the µH range, therefore a few turns (three to eight) are sufficient. These coils are manufactured either by using a coil winding process or a wire embedding process [4].

This range of frequencies (50 kHz – 150 kHz low frequency induction and 2 MHz –20 MHz high frequency induction) has the following advantages/drawbacks:

- ➢ Advantages
  - ♦ Control of the communication area. It means you can shape the zone where a transaction will occur.
  - ♦ Little sensitivity to external interference.
  - ♦ Unaffected by the human body.
- ➢ Drawbacks
  - ♦ Low bit rate compared to microwave
  - ♦ Range much smaller than microwave.

The high frequency induction has a higher bit rate than the low frequency induction [2].

Cards operated at 13,56 MHz

As already said inductive coupling contactless cards communicate with the IFD using a technique called load modulation where the card changes its load (for example a resistor), which is sensed by the reader.

Contactless cards which operate at 13,56 MHz use different types of modulation and different types of coding, but take into account only the modulation standardised by ISO/IEC : we speak about the Proximity Integrated Circuit Cards (PICC) and Vicinity Integrated Circuit Card (VICC)

PICC are described by the ISO/IEC 14443 standard series. The standard defines two possible modulations called Type A and Type B. Both Type A and Type B use Amplitude Shift Key (ASK) modulation for communication between the reader, called Proximity Coupling Device (PCD), and the card.

PCD ➔ PICC Communication

Type A uses the modulation principle of ASK 100% of the RF operating field to create a “Pause”. The bit coding is done with the Modified Miller code which enables to define three sequences used to code the following information:

- Logic “1”
- Logic “0”
- Start of communication
- End of communication
- No information

This allows Type A cards to count the bits of a frame and to identify an error in the frame even without any parity or CRC checking [6].

Type B uses the modulation principle of ASK 10% of the operating field. The bit coding is done with a Non Return to Zero coding which doesn’t offer different bit representations for logic “1”, logic “0’ and “No information”.

PICC ➔ PCD Communication

Both Type A and Type B cards are able to communicate with the PCD via an inductive coupling area where the carrier frequency (13,56 MHz) is loaded to generate a sub-carrier with frequency of ~847 kHz. The sub-carrier is obtained by switching a load in the PICC.

Type A cards modulate the sub-carrier using On-Off Keying[1] (OOK) modulation. The bit coding is done with the Manchester coding which enables to define three sequences used to code the following information:

- Logic “1”
- Logic “0”
- Start of communication
- End of communication
- No information

Type B cards modulate the sub-carrier using Binary Phase Shift Keying (BPSK) modulation. The bit coding is done with a Non Return to Zero where the change of logic level is denoted by a phase shift (180°) of the sub-carrier.

Type A and Type B communicate in either direction (PCD to PICC and PICC to PCD) at the rate of 106 Kbytes/s.

Anticollision

To avoid interference between two or more contactless cards in the PCD range, it is necessary to define a protocol which manages the collisions between them. This protocol is called Anticollision and is used to establish a link between the PCD and only a single card, within a short time.

[1] OOK modulation is an ASK particular case where the amplitude lessening is infinite.

The following state diagram helps understanding the anticollision loop principle for Type A cards:

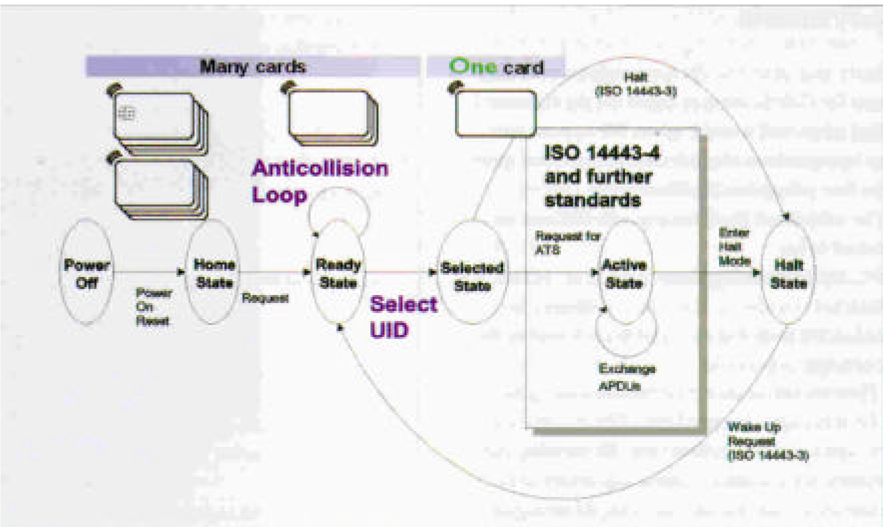


Figure 5 - State diagram for Type A cards [7]

Home State: this state is entered after power on and left after a request

Ready State: this state is entered after a request and maintained; it is left when the PICC is selected with its serial number called Unique ID (UID).

Selected State: this state is entered by selecting the PICC with its complete serial number. From this state there are two possible state transitions:

Active State: in this state actions like PTS and exchange of APDU may be performed.

Halt State: in this state PICC shall respond only to a wake-up request. There are two ways to enter this state:

1. Due to a transition from *Selected State* via the halt-command
2. Due to a transition from *Active State* via APDU

A wake-up request moves the PICC to *Ready State*.

PICCs that remain in *Halt State* will not participate in any further anticollision loop when a standard request is applied. This reduces the number of cards in the anticollision loop, increasing the anticollision procedure speed.

Type A cards use three types of frames in order to communicate with the PCD. The first one is the *Request and Wake-up Frame* which is used to initiate communication; this frame has a different structure from the other two, so a PICC can reliably identify a request. The second one is the *Standard Frame*, which is used for data exchange. The last one is the *Bit-oriented Anticollision Frame* which is used only during anticollision loops.

Thanks to Modified Miller coding and because the card answers synchronously to request commands with Type A PCD, it is possible to detect a collision at bit level (see Figure 6).

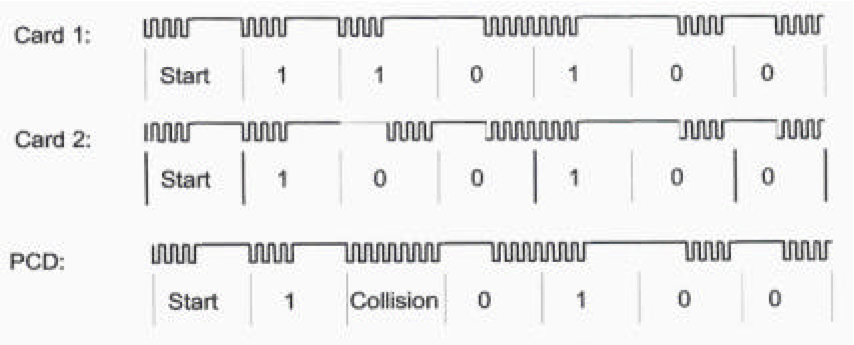


Figure 6 - Bit collision detection principle used by Type A cards [7]

As the aim is to find a serial number as fast as possible and afterwards select the card, the following method is used to avoid collisions:

PCD **PICC**

Give me your UID →

← PICC1 send UID e.g. 01010111…

← PICC2 send UID e.g. 01110111…

← PICC3 send UID e.g. 01010100…

The PCD sees the following data stream (C=collision): 01C101CC…

The PCD knows that the first collision is at position 3: all others are ignored at this stage. The PCD sends a select command again requesting only cards which have a serial number starting with 01 plus, instead of the first occurrence of a collision, a 1.

Select cards with serial number starting with 011 →

PICC with serial number starting with 011 will answer with the remaining bits of their serial number

PICC1 remains silent

← PICC2 send rest of UID 1011110…

The PCD knows the PICC2 serial number and sends a final Select command

Select card with UID 01110111… →

← PICC2 acknowledges selection

Type B cards use NRZ coding where “no information” and “information” cannot be distinguished, furthermore they are not bit synchronous, so it is impossible to detect a collision at bit level. Collision detection is based on communication errors produced by multiple cards in the operating field and such errors are detected using Cyclic Redundancy Check (CRC) checking. In order to better understand the Type B anticollision procedure it is important to define the characters and the frame format used during communication between PICC and PCD.

Bytes are transmitted and received between PICCs and a PCD by characters, the format of which during the Anticollision sequence is as follows :

- 1 start bit at logic "0" ;
- 8 data bits transmitted, LSB first ;
- 1 stop bit at logic "1".

PCDs and PICCs shall send characters as frames. The frame is normally delimited by Start Of Frame (SOF) and by End Of Frame (EOF). A frame shall only be considered correct if it is received with a valid CRC_B value. The frame CRC_B is a function of k data bits, which consist of all the data bits in the frame, excluding start bits, stop bits, delays between bytes, SOF and EOF, and the CRC_B itself. Since data is encoded in bytes, the number k of bits is a multiple of 8.

An anticollision sequence is managed by the PCD through a set of commands detailed in this section. The PCD is the master of the communication with one or more PICCs. It initiates PICC communication activity by issuing a Request Command to prompt for PICCs to respond.

During the anticollision sequence it may happen that two or more PICCs respond simultaneously : this is a collision. The command set allows the PCD to handle sequences to separate PICC transmissions in time. The PCD may repeat its anticollision procedure until it finds all PICCs in the operating volume.

Having completed the anticollision sequence, PICC communication will be under control of the PCD, allowing only one PICC to talk at a time.

The anticollision scheme is based on the definition of timeslots in which PICCs are invited to answer with minimum identification data. The number of slots is parameterised in the Request Command and can vary from one to some integer number. PICC response probability in each timeslot is also controllable. PICCs are allowed to answer only once in the anticollision sequence.

Consequently, even in case of multiple PICCs present in the PCD field, there will probably be a slot in which only one PICC answers and where the PCD is able to capture the identification data. Based on the identification data the PCD is able to establish a communication channel with the identified PICC.

An anticollision sequence allows selection of one or more PICCs for further communication at any time. The set of commands allows implementation of different anticollision management strategies at the PCD level. This strategy is under the control of the application designer and can be :

- probabilistic (repetitive single slot prompt with response probability less than or equal to 1) ;
- pseudo-deterministic (multiple slots with scanning of them during the anticollision sequence to have the maximum probability that all present PICCs answer) ;
- any combination of these methods that can be conducted dynamically.

If more than one PICC is in the PCD RF field a first choice can be done by means of the Application Family Identifier (AFI). AFI represents the type of application targeted by the PCD and it is contained in the Request Command. Only PICCs with applications of the type indicated by the AFI may answer to a Request Command.

After receiving a valid Request Command a PICC shall respond according to the following rules, where the parameter N has been given in the Request Command :

- If N = 1 the PICC shall send an Answer To Request Command and is ready to start the communication
- If N > 1 the PICC shall internally generate a random number R which shall be evenly distributed between 1 to N
  - If R = 1 the PICC shall send an Answer To Request Command and is ready to start the communication.
  - If R > 1 the PICC shall wait for another Request Command or for a Slot Marker Command which defines the time slot for it.

The following example may clarify the Type B anticollision procedure:

PCD	PICC
REQB (AFI=10 and N=1) →	
	← PICC 1 Matched AFI, N=1, transmit ATQB
	PICC2 Unmatched AFI, wait for next REQB
	← PICC3 Matched AFI, N=1, transmit ATQB
Collision detected, REQB (AFI=10 and N=4) →	
	PICC1 randomly selects R between 1 and N: R=2 so wait for slot marker for slot 2
	← PICC 3 randomly selects R between 1 and N: R=1 so transmit in ATQB in slot 1
PCD has now a choice depending on its application: select the PICC3 and send no more slot markers, continue sending slot markers, or other possibilities.	
For this example the PCD will continue to send slot markers.	
Slot Marker for slot 2 →	

🡐 PICC1 R=2 transmit ATBQ in slot 2

Now the PCD has received two PICC responses and can decide which card to select in order to continue the communication.

VICC are described by the ISO/IEC 15693 standard series. In order to meet different international radio regulations and different application requirements, different modes and different data coding have been defined in the standard which can be combined with any modulation.

VCD ➔ VICC Communication

The communication between the Vicinity Coupling Device (VCD) and the VICC takes place using the modulation principle of ASK. Two modulation indexes are used, 10% and 100% and the VICC shall be able to decode both.

Data coding shall be implemented using pulse position modulation. Two data coding modes shall be supported by the VICC. The selection shall be made by the VCD and indicated to the VICC within the start of frame (SOF). The data coding modes are called “1 out of 256” and “1 out of 4”; the first one represents the value of one single byte with the position of 1 pause of 256 successive time period of 256/f_c. In the example of Figure 7 data 'E1' = (11100001)b = (225) is sent by the VCD to the VICC.

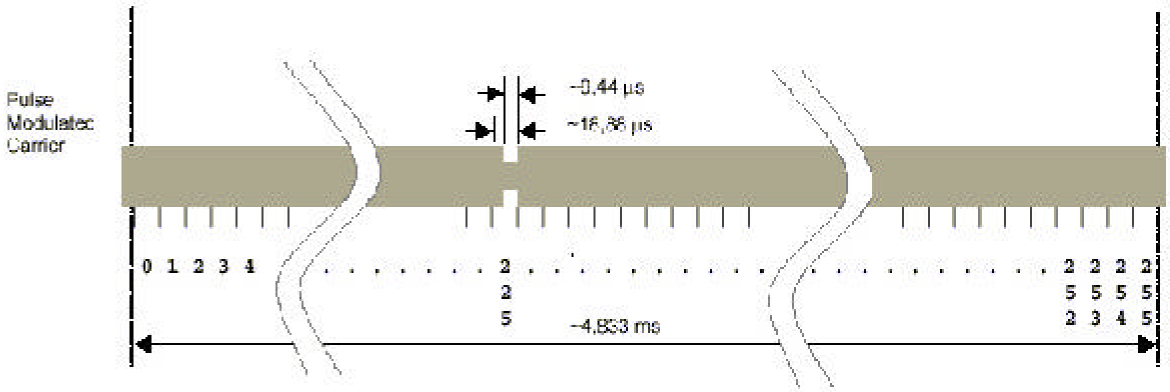


Figure 7- 1 out of 256 coding mode

In the second mode the pulse position determines two bits at a time defining four different pulses associated to the bit pairs “00”, “01”, “10” and “11” (see Figure 8).

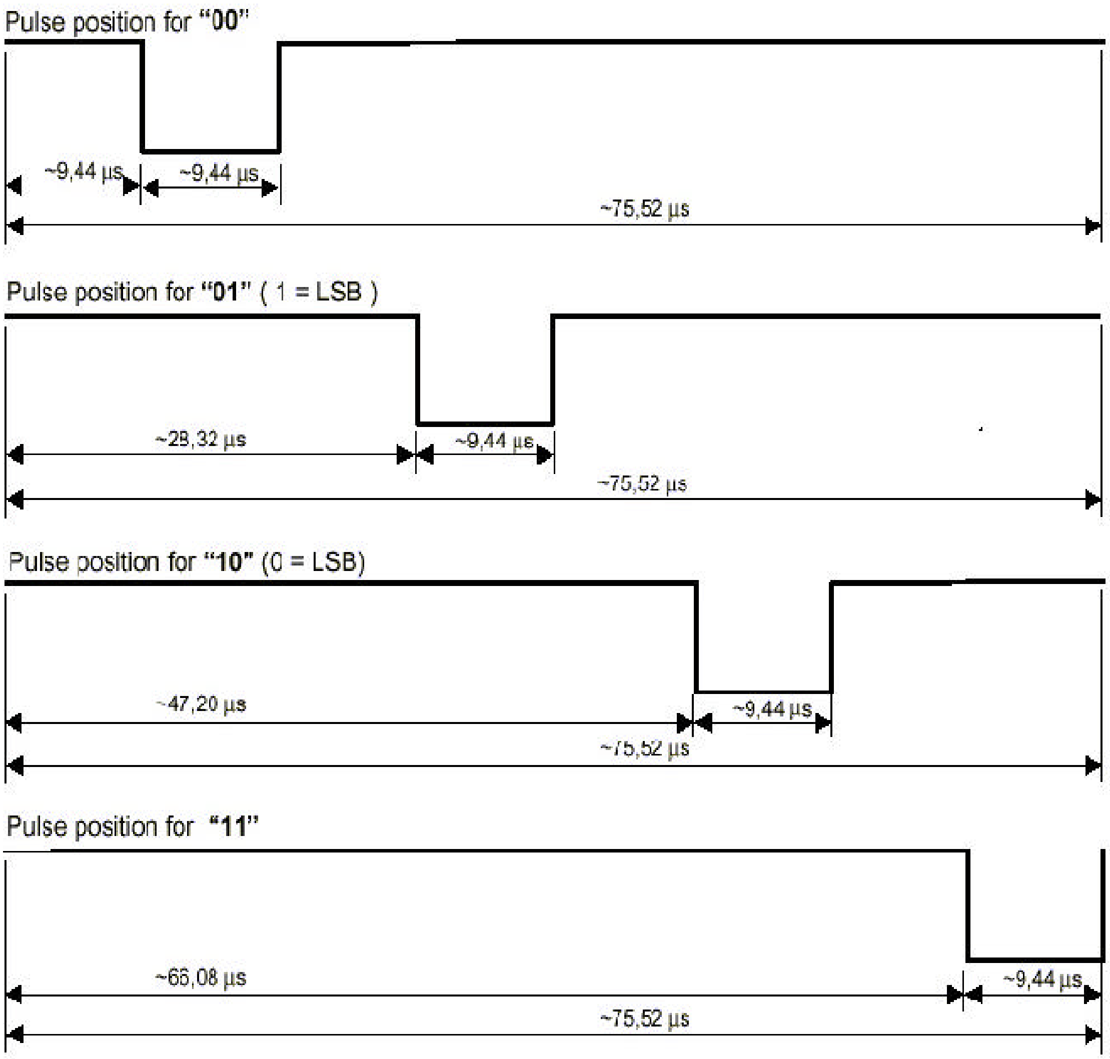


Figure 8 - 1 out of 4 coding mode

For example Figure 9 shows the transmission of 'E1' = (11100001)b = 225 by the VCD.

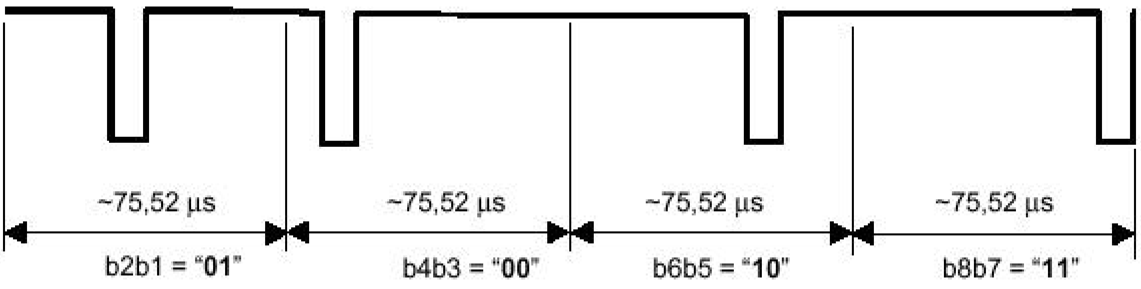


Figure 9 - 1 out of 4 coding example

To grant ease of synchronisation and independence of protocol for the VCD to VICC communication, it was decided to use a frame. Frames shall be delimited by a start of frame (SOF) and an end of frame (EOF) and are implemented using code violation.

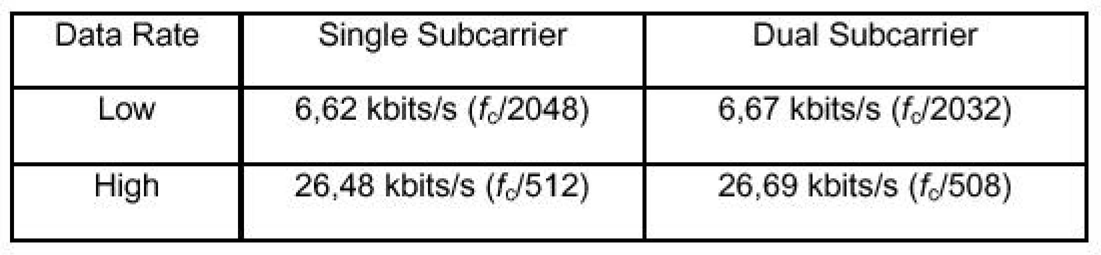
VICC → VCD Communication

The communication between VICC and VCD takes place using Load Modulation. The VICC shall be capable of communication with the VCD via an inductive coupling area whereby the carrier is loaded to generate a sub-carrier with frequency f_s. The sub-carrier shall be generated by switching a load in the VICC.

One or two sub-carriers may be used as selected by the VCD. When one sub-carrier is used, the frequency f_{s1} of the sub-carrier load modulation shall be f_c/32 (423,75 kHz). When two sub-carriers are used, the frequency f_{s1} shall be f_c/32 (423,75 kHz), and the frequency f_{s2} shall be f_c/28 (484,28 kHz).

The VCD can select a low or a high data rate (see Table 1), but the VICC shall support both.

Table 1 - Data rates



Data Rate	Single Subcarrier	Dual Subcarrier
Low	6,62 kbits/s (f_c/2048)	6,67 kbits/s (f_c/2032)
High	26,48 kbits/s (f_c/512)	26,69 kbits/s (f_c/508)

Data shall be encoded using Manchester coding and, as in the communication from VCD to VICC, it is structured in frames delimited by a start of frame (SOF) and an end of frame (EOF) and is implemented using code violation.

Anticollision

The VICC are Uniquely IDentified by a 64 bits unique identifier (UID). This is used for addressing each VICCs uniquely and individually, during the anticollision loop and for one-to-one exchange between a VCD and a VICC. Moreover the VICCs may also (optionally) have an AFI (Application family identifier) which represents the type of application targeted by the VCD and is used to extract from all the VICCs present only the VICC meeting the required application criteria. The AFI coding is defined in the ISO/IEC 15693-3.

The purpose of the anticollision sequence is to make an inventory of the VICCs present in the VCD field by their unique ID (UID). The VCD is the master of the communication with one or multiple VICCs and thanks to an algorithm which manages different time slots, it is able to understand the UID and the AID of the VICCs within its field.

Capacitive Coupling

Capacitive coupling involves placing a pair of conductors below the surface of the smart card. When a voltage signal is placed across them, a charge separation occurs that generates an electric field. The electric field can extend beyond the surface and induce another charge separation on a second pair of conductors in the read/write unit, which transmits data between the card and the read/write unit. The advantages of this technique are that digital information can be transferred directly and no modulation is required.

One example of this type of contactless card is the Contactless Integrated Circuit(s) Cards (CICC) standardised in the ISO/IEC 10536. The standard defines both the inductive and the capacitive interface, but here we describe only the capacitive coupling.

The CICC has four coupling areas, one pair is used for communication from CICC to the CCD and the other pair is used for communication from CCD to CICC. The pairs of capacitive coupling areas have a differential relationship, in fact their polarity shall alternate with respect to their adjacent areas.

The communication between CDC and CICC takes place without modulation, so only data coding is necessary. The coding technique for capacitive data transfer shall be differential NRZ.

When the CICC is put in contact with the CDC, it shall send its answer to reset on one of the two pairs of capacitive plate, in order to define the communication channel for communication from CICC to the CDC. The answer to reset is also used to determine the orientation of the card, if necessary.

No anticollision technique is necessary since only one card at a time can physically be in contact with the interface device.

3.4 Supports

Integrated Circuit(s) Cards without contact are standardised by ISO/IEC which has defined three types of cards:

- Contactless Integrated Circuit(s) Cards (CICC)
- Proximity Integrated Circuit(s) Cards (PICC)
- Vicinity Integrated Circuit(s) Cards (VICC)

All the cards are based on the ID-1 format described in the ISO/IEC 7810 standard and contain an antenna embedded in the PVC layer which forms the card. If the CICC is able to communicate in a capacitive way it contains also four capacitive plates used for data transmission and reception (see previous subsection).

Currently there are three basic antenna types on the market: wired, etched and printed. The first uses regular copper wire similar to 125 kHz antennae, only thicker. There are two manufacturing methods for wired antennae, the former is the same coil winding process as for 125 kHz the latter is a wire embedding process similar to a plotter, where the wire is essentially “written” into the plastic substrate.

Etched antennae are produced in the same way a regular PCB would be made. A layer of 35 µm of copper is etched in the shape of the antenna. In recent years, the electrical parameters were inferior to wired antennae, but lately the parameters have come to a competitive range. However, crossover are still awkward to manufacture at this time.

Printed antennae employ conductive ink, that is silkscreen printed on the sheets. The electrical parameters of those antennae are still inferior to wired antennae.

Another topic in the contactless card manufacturing process which is absent in the normal contact card manufacturing process is the interconnection between the chip module and the antenna.

Currently there are five principal interconnection methods a card manufacturer needs to understand and choose from:

- Thermal compression bonding
- Soldering
- Conductive gluing
- Crimping
- Ultrasonic welding

Thermal compression bonding employs temperatures of 1500ºC and higher while simultaneously applying pressure to interconnect the wire with the chip module. This is a solid state interconnection, where free electrons from the wire migrate into the chip module substrate, and vice versa, to form a new crystal at the point of interconnection. The ohmic resistance is the lowest of all five interconnection methods.

There is no need to get rid of the isolation before the interconnection, which is an additional advantage of this process: it is simply burnt away during the process. This is a true electrical interconnection and is mainly used for wired antennae.

In the **Soldering** method a third material (tin) is introduced to mechanically interconnect the wire with the substrate. This method is mainly used for etched antennae.

In the **Conductive gluing** method a conductive glue provides the electrical interconnection between the ends of the antenna and the chip module.

The **Crimping** method forces a metal pin through the chip module and mechanical force is used to crimp the ends of the antenna to the chip module. This method is sometimes found with etched inlay.

In the **Ultrasonic welding** method an ultrasonic tool provides the heat and the pressure for this interconnection method. The temperature for this process is far less than the one used with thermal compression bonding. This is again a mechanical interconnection.

In summary, today the most widespread technology choice for the production of 13.56 MHz contactless memory cards is wired embedded antennae interconnected to the chip module with thermal compression bonding methods, in order to grant both performance and quality [4]. However this choice may be different for dual interface cards as thermal compression bonding may not always be applicable for this kind of cards.

3.5 Standards

ISO and IEC work together in the field of Information Technology thanks to the Joint Technical Committee 1 (JTC1). The standardization activity on cards and personal identification field is done by the Sub Committee 17 (SC17). Inside the SC17 there are three working groups related to the IC Cards:

- WG1 - Physical characteristics and test methods for ID-cards
- WG4 - Integrated circuit cards with contacts
- WG8 - Integrated circuit cards without contacts

In this document we focus on WG8 which is the group concerning Contactless Cards standardisation.

WG8 has delegated its projects to three subgroups to achieve efficient and dedicated developments of the standards. For the development of the standard series ISO/IEC 14443 the subgroup WG8/TF2, or shorter just TF2, standing for Task Force 2, was established in 1994. For the development of the standard series ISO/IEC 15693 the subgroup WG8/TF3, or shorter just TF3, was established in 1996. There is one more Task Force, namely TF1, which was established in 1990 and was originally developing the standard ISO/IEC 10536. It still exists, but has presently no specific development task [8].

Table 2 - WG8 Standards

Spec	Title	Year	Under Revision
ISO/IEC 10536-1	Identification cards - Contactless integrated circuit(s) cards - Close-coupled cards - Part 1: Physical characteristics	2000	No
ISO/IEC 10536-2	Identification cards - Contactless integrated circuit(s) cards - Part 2: Dimensions and location of coupling areas	1995	No
ISO/IEC 10536-3	Identification cards - Contactless integrated circuit(s) cards - Part 3: Electronic signals and reset procedures	1996	Yes
ISO/IEC 14443-1	Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 1: Physical characteristics	2000	No
ISO/IEC 14443-2	Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 2: Radio frequency power and signal interface	2001	No
ISO/IEC 14443-3	Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 3: Initialisation and anticollision	2001	No
ISO/IEC 14443-4	Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 4: Transmission protocol	2001	No
ISO/IEC 15693-1	Identification cards - Contactless integrated circuit(s) cards - Vicinity cards - Part 1: Physical characteristics	2000	No
ISO/IEC 15693-2	Identification cards - Contactless integrated circuit(s) cards - Vicinity cards - Part 2: Air interface and initialisation	2000	No
ISO/IEC 15693-2 Cor 1		2001	No
ISO/IEC 15693-3	Identification cards - Contactless integrated circuit(s) cards - Vicinity cards - Part 3: Anticollision and transmission protocol	2001	No

The standard series listed above cover the description of the physical, electrical and logical components of the three types of IC Contactless Cards. Table 3 summarizes the main differences between them.

Table 3 - Contactless Card Types

Card Type	ISO Standard	Range	Application Field
Close Coupled CICC	10536	1 mm	Contact Cards alternative
Proximity PICC	14443	5 cm	Physical access, payment, High security applications
Vicinity VICC	15693	1 m	Physical access, lower security applications than Proximity

4 State of the art in Security

In this section we review the current status in security both for contact and contactless card technology. An overview of the basics of smart card technology is given in [9].

4.1 State of the art in security for contact cards

The security of smart cards is a fast evolving domain.

Today, specialists distinguish between 3 different targets for which several attacks and countermeasures may be listed:

a) A smart card is first composed of **a silicon chip**, which is an embedded piece of hardware. Thus any kind of invasive or non invasive attack on the hardware has to be taken into account when evaluating a smart card.

b) On top of the hardware architecture, the **operating system** or the **software layers** contained in the microprocessor card may provide an interesting target for the hacker. These have to be protected against several known mechanisms.

c) Finally, the last layer which has to be taken into account is the **application level**. The cryptography needs to be done the right way, and the system has to be evaluated in the information security sense.

Hardware Security

Attacks on hardware parts of the chip may be both *invasive* and *non invasive*.

Invasive attacks are the most powerful ones known to date. For example a malicious person may deposit probe pads on the data bus or through the conductive grid, expose hardwired ROM (Read-only memory) links, defeat blown fuse links, connect tracks, or even cut tracks. All the examples lead to a modified behaviour of the chip, which can result in a security breach.

For example probing pads can further be observed via an electronic microscope and individual bit values may be read out of memory or from the data bus. Typical tools such as focused ions beams enable to drill holes through the metal layers of the chip to observe some deeply buried links or memory parts.

The circuit may be modified in the chip in order to achieve a specific goal: for example disconnect any security sensors contained in the metal layers, or disconnect the random number generators in order to keep them stuck at a fixed value, etc.

Fuse is blown.

Component is in User Mode

FIB Station

Fuse is regenerated.

Component is back to Issuer Mod

These attacks are not specific to a smart card. It is important to note that an attack on the chip requires an important investment in time and resources, sophisticated and expensive tools and a good hardware expertise.

Another idea is to apply voltage or frequency variations on the external contacts of the chip in order to generate computation faults which may in specific cases reveal secrets stored in the card (see paragraph on side-channel attacks). Furthermore, environmental conditions such as temperature may be changed, or x-rays, light pulses or microwaves may be applied to the chip in order to generate a strange behaviour or deactivate protecting shields on the chip.

The list of sensitive items on the chip which should be carefully protected includes (but is not limited to):

Security Sensors, Internal Clock, Reset, Design & Layout, ROM, RAM, EEPROM, CPU, data and instruction buses, Random Number Generators, Memory Management Unit, Crypto-Coprocessor.

Several techniques can be applied to prevent hardware attacks. These include ciphering and scrambling memory cells, using error correction codes or checksums on intermediate or transmitted data, burying very sensitive items such as the data buses or the random number generator under several layers of independent metal masks, disconnecting the clock from the external supply and using an internal free running oscillator and using all kinds of security sensors to detect fraudulent manipulation of the chip.

Embedded Software Security

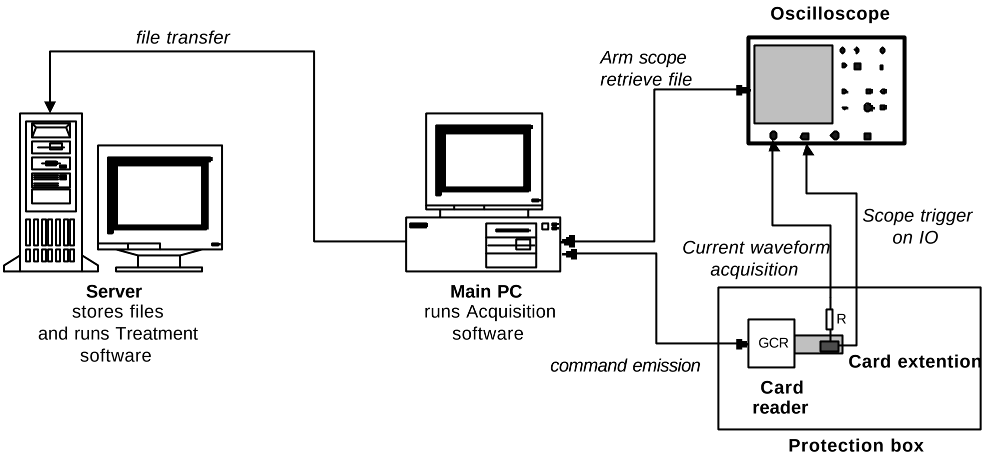
Attacks on the software part or the operating system of a smart card are mostly performed by logical means.

Side-Channel analysis [12] is a form of attack against secure tokens by which secret data is pulled out without damaging the device itself. By monitoring the execution time [10], the power consumption [13][14][15] or the electromagnetic radiation [16][17] of a Smart card Integrated Circuit, it is frequently possible to infer information about the processed data. Performing a Side-Channel analysis on a secure token requires a sound knowledge in electronics, cryptography, signal processing and statistics. A now well known class of attack in this group is based on smart card power consumption analysis : **D**ifferential **P**ower **A**nalysis (DPA) and **S**imple **P**ower **A**nalysis (SPA), but also on timing analysis.

The concept of **SPA** consists in observing the variations in the global power consumption of the chip and retrieving from it some information that can help to identify any secret. For example, an increase in power consumption might indicate where a modular exponentiation is performed. In general, a SPA will give better results if the hardware architecture is known.

The **DPA** is more sophisticated than the SPA: it consists in performing a statistical analysis, on power consumption curves, of several executions of the same algorithm with different inputs to retrieve the information.

The following figure shows an acquisition platform for SPA, DPA side channel analysis:



The **timing attacks** were a main issue in the past because several optimisations implied algorithms with varying timings depending on the data and/or the cryptographic keys being used. All the current implementations have to be designed with constant timing; at least not depending on data and secret keys.

A newer attack is the **Electromagnetic Analysis** it is based on the same techniques used for DPA and SPA, but the measured physical quantities are different. In this case, it is the RF signals that are interesting. While also being a side-channel attack, Electromagnetic attacks differ in a number of crucial points from power attacks.

In short, since any electrical current flowing through a conductor induces electromagnetic (EM) emanations, it seems natural to look for the same phenomenon in the vicinity of a semiconductor. As the power consumption of a tamper-resistant device varies while data are being processed, so does the EM field and one may legitimately expect to extract secret information from a relevant EM analysis.

In some cases, power curves appear to convey no information: this happens when power does not vary or does vary but in a way seemingly de-correlated from the secret data. Very much simplified, the chip's global current consumption can be looked upon as a big stream concentrating the sum of the small tributaries flowing into it. If the sub-components' contributions could be determined, then the small streams would be isolated. This is impossible by direct electrical measurement but is possible by eavesdropping local EM radiation. By opposition to power analysis, this requires the design of special probes and the development of advanced measurement methods that focus very accurately selected points of the chip.

EM's advantage is definitely its capability of exploiting local information. This geometrical degree of freedom is useful as it allows pinpointing the problematic spots that leak information. Power attacks' major advantage is undoubtedly the relative simplicity of electric measurements as opposed to EM ones.

Fault Attacks [11] consist mainly in applying a combination of environmental conditions that causes the card chip to produce a wrong computation that can leak secret information concerning any information in the card. Abnormal working conditions sensors are therefore necessary to avoid huge software and hardware countermeasures. It is always better anticipating than correcting errors.

Application Security

Application level attacks are attacks focusing on flaws using the normal communication channel to interface with the card. These flaws potentially lower security features of the card or allow to bypass them and fraud the system. There is a wide range of such attacks, some of them being non specific to the smart card. For example, wrong file access conditions, malicious code, flaws on cryptographic protocols, design or implementation are common flaws to any computing systems.

4.2 Potential vulnerabilities of contactless products

Smart cards based on contact technologies have been largely spread in the field and, in most cases, their security level has been assessed before their deployment in volumes.

Even if it is evolving rapidly, the security of contact-based technology (its assets and its potential weaknesses) is well known by the main key actors: application providers, chip designers, operating system developers, third party evaluators and researchers.

The same interest is growing in the field of contactless-based products. Due to the specific features of this technology, its operating modes and its constraints, a dedicated vision shall be built and shared between users of contactless technology and product makers.

Security at transaction level

Since a contactless card can be operated without the consent or awareness of the cardholder, the threat that a thief establishes a covert transaction with a legitimate card needs to be analysed.

This is theoretically possible since public standards define how information shall be transmitted over the air.

Nevertheless, the attacker needs to manufacture a fake reader in order to exploit this potential threat.

To increase the difficulty of producing such fake readers, we can consider using techniques based on strong cryptography, for instance by mandating cards and readers to do a mutual authentication, preliminary to any transaction.

Another threat resides in the fact that an attacker can intercept data exchange in order to observe or modify some parts of the messages.

This type of attacker is often referred to as “ man in the middle” attacks.

This threat can also be countered efficiently using data protection techniques based on strong cryptography

- Encryption techniques, to ensure data confidentiality (e.g. when loading a secret key into the card)
- Signature techniques, to ensure data integrity (e.g. when transmitting the amount of a financial transaction)

However, it is possible that some applications cannot afford strong cryptography because this would go against other objectives (performances, costs).

That is why an evaluation of the risk related to the threats exposed hereafter is necessary.

Timing attacks

As learnt from contact technology, the observation of communication channels may be of great interest for attackers.

Firstly, any differences in the timings of the card's responses could expose a secret data (e.g. during PIN code verification).

Secondly, any event observable on the communication line can be used as a reference to trigger more sophisticated attacks (observation of covert channel or perturbation of card operations).

What is the status in contactless technology?

Data are exchanged on the radio-frequency interface, using amplitude or charge modulation techniques. Equipment necessary to capture data on this interface is accessible with limited budget and can be used with limited technical expertise.

Thus, potential timing attacks apply to contactless technology.

Products should be protected, using, for instance, the countermeasure principles that have proved their efficiency in the contact world.

Signal manipulations

From the contact-card experience, we know that one of the most basic attack scenarios consists in injecting perturbed signals in the smart card, typically through power supply and clock inputs.

The attacker's goal is to induce misbehaviours in the smart card's operating system that he can exploit to get access to unauthorised data or services (e.g. by hijacking the verification of access rights assigned to sensitive information fields).

We also know that a proper monitoring of these signals, with or without the assistance of the operating system, is, in most cases, sufficient to eliminate any security risks.

Contactless chips are powered and clocked by the reader through the radio-frequency interface. To do so, they incorporate power and clock generation units that shall take into account some operational constraints: the coupling shall be functional as long as the card remains below a distance of 10 cm from the reader, whatever the geometric position of the chip's antenna. They must also take into account that the card can move in the working area.

This implies that contactless chips present some flexibility regarding the way they are operated. It might have two impacts on security, summed up by the two following questions:

- How difficult is it for an attacker to generate efficient perturbation scenarios from the radio frequency interface?
- How easy is it for chip suppliers to filter potentially dangerous perturbations and to monitor the correctness of operations within the chip?

The vision of contactless security includes some answers to both questions.

Side channels

Powerful non-intrusive attacks against smart cards are based on the observation of side channels.

Well-known attacks use, for instance, the dependency between the secret data manipulated by the chip and the power consumed during the manipulation of such data.

Many laboratories have proved the efficiency of these attacks on contact-based products, which did not incorporate ad hoc countermeasures.

For instance, recall that in 1998 a method called DPA (Differential Power Analysis) was discovered, which deduces secret keys by calculating how much electrical current measured on the VCC Pad correlates with intermediate results of calculations performed during a cryptographic process.

These attacks are theoretically possible on contactless products as the power consumption can still be measured from the emitted field.

Another idea, applicable to products combining contact and contactless technologies, would be to measure information leakage on the contact's VCC pad during an RF-operated transaction.

4.3 Issues for securing contactless technology

Processing Speed

Applications using contactless technologies require that the duration of a single transaction does not exceed 150 ms to 200 ms, seen from the user's point of view.

This timing includes the following steps:

- Session establishment between card and reader, anticollision mechanisms representing a major part of this step.
- Data transportation between card and reader (the typical pace is 106k bits per second).
- Data processing within the card and within the terminal.

This constraint does not open any new vulnerability that attackers could try to exploit but are likely to reduce the possibilities in securing contactless cards as lots of countermeasures imply longer processes (stronger cryptographic schemes, redundancy checks, dummy processes, ...).

One major challenge for product designers is to develop more efficient cryptographic schemes respecting the requirements of contactless applications.

However, it shall be kept in mind that the duration of the whole transaction depends mainly on the application itself (volume of data exchanged, for instance) and that this issue can only be addressed with a global view.

Power Consumption

Typically, current products based on contactless technology consume a power ranging between 2 mW and 5 mW.

Our experience in contact technologies shows that power analysis attacks can be made more difficult by adding noise to the current consumption patterns. This forces the attacker to record more data in order to eliminate this noise.

An effect of this kind of countermeasure is to increase the power consumption. Applying this kind of securing technique in the contactless world should therefore be considered with great caution.

4.4 Conclusion

The first objective is to evaluate whether contactless technology presents any specific vulnerability regarding covert sessions, man-in-the-middle, fault injection and side channel analysis.

The second objective is to evaluate the feasibility of efficient protective techniques against potential weaknesses.

The next section reviews potential threats that may apply to contactless technology in somewhat greater detail and proposes possible solutions where applicable.

5 Specific threats in contactless technology

Chip and hardware technology do not depend much on the card being contact or contactless.

However, the fact that an RF link is involved, and that the communication between the card and the reader differs from contact technology, may open venues for new attacks and threats specific to our case.

Another important aspect for contactless cards is the system around the card, and more specifically the application based on the card. In many cases, new threats related to specific applications may arise and have to be seriously taken into account.

In this section, we detail the global threat categories that we have been investigating, and, where possible, we describe potential vulnerabilities but also potential countermeasures for attacks on contactless cards and applications.

5.1 Eavesdropping

Obviously, eavesdropping is the most common threat on contactless technology users. As the communication takes place over the radio frequency link rather than through direct contact between the chipcard and the terminal, an adversary can easily intercept and listen to the communication without the legitimate user or the terminal being aware of it. This could lead to unwanted disclosure of information held on the card and which the user might not want to see published.

Encryption of the communication between the card and the reader is thus mandatory to provide security against passive eavesdroppers.

A particular example of such attacks where the information needs to remain confidential is when the user authenticates himself to the card via a pinpad located on the terminal. The trial PIN value sent from terminal to card to check the identity of the legitimate user necessarily has to be encrypted.

In the active setting, an adversary may even insert blocks of data between the terminal and the reader, or cut parts of the communication or even replace parts by other data. This is referred to as the *man-in-the-middle* attack and is particularly meaningful in the contactless context as the user may not even be aware of the presence of such an active attacker. This threat may be thwarted by encrypting and authenticating the communication channel between the card and the terminal, using secure messaging techniques which also exist in the contact card world.

5.2 Operation Interruption

Another particular threat in the context of contactless technology lies in the fact that the system never knows when the user is going to interrupt the operation. The action of taking the card out of the electromagnetic field is therefore not an abnormal action anymore, and may happen at any time.

It is up to the application (in the card or in the terminal) to ensure that such interrupts do not compromise ongoing transactions. Backup mechanisms or equivalent mechanisms have to be implemented to ensure a transaction comes to a regular end.

In contrast to contact cards, in a contactless setting, either the card or the reader needs to make sure the transaction went well all over, but the risk associated with this threat should in any case be endorsed by the system. For example, suppose a user is granted access to a public transportation means via his contactless card, and suppose further on that after being debited on his card, the access is not granted say because of a mechanical failure of the doors. In this case, the reader should verify that the transaction has not been ratified and duly restore the credit on the card. In any case, access should be granted without the card being debited again.

5.3 Denial of Service

A rather generic class of threats is the *denial of service* class.

Every card is vulnerable to different attacks in which the goal of the adversary is simply to disable the communication between the card and the terminal in some way, or to interrupt the operation of the card at a crucial point in time, or even worse to use the card without the legitimate user being aware of it in order to disable subsequent services the card could offer to the user.

A simple countermeasure could be to add terminal certificates to the application in order for the card to be able to check whether it is communicating with a legitimate terminal. However this does not protect against fraudulent terminals as we shall see in the next paragraph.

On the other hand, denial of service attacks on readers are far more difficult to mount in the contactless case than to disable a contact reader to operate normally by say blocking the slot where the user introduces his card.

5.4 Remote card destruction

Another very simple threat consists in destroying the card at a distance by sending inappropriate waves to the card or by exposing it to a damaging electromagnetic field, still without the legitimate user noticing it.

A fraudulent user may also decide to destroy the card himself in order to claim reimbursement of lost credit units or tickets. He may for example start using the card normally until all but a few units are gone, and then decide to disable the card in order to claim the whole service once more. It is then much harder for the issuer to decide whether, or even to prove that, the user has been tampering with the chip than for contact cards.

Physical destruction of the contact card is far more obvious than destruction of the RF interface of contactless cards.

5.5 Card theft

It is much harder to steal a card from a legitimate user because during contactless transactions the user never really gives his card away. In contact technology, the user is often asked to hand over his card to the merchant to realise the transaction.

5.6 Card cloning

After recovering all valuable information stored in the card by eavesdropping or other means, an attacker usually intends to build a valid clone of a valid card. In contactless technology applications, there usually exist visual means and control methods to ensure a card is not a clone. For example, in public transportation, controllers may ask users to show their card and apply an additional identity check such as having a picture on the card or having it contain an ID number corresponding to a picture ID. In contact technology, simpler methods such as controlling the card thickness via the reader slot are used to help overcoming the cloning problem. However, visual controls are much less common than for typical contactless card applications.

5.7 Surreptitious Card Operation

A typical example of such attacks is a fraudulent merchant engaging into a communication with the card without the user knowing about it. The merchant could then proceed to debit a few credit units at a time, when the user thinks he is paying only one credit. The service offered by the card is thus much more expensive than expected and the card may not work any more after a certain period of time because all credits will have vanished from the user's account.

From the attacker's point of view, the merchant can either choose to debit units for which he will not have to provide a service any more, or on the contrary increment some credit he will collect later on from the financial organisation. In this latter case for example, in order to fool the user, he could first write a huge transaction, followed by a smaller one which the user sees on the terminal before giving his approval for the operation.

5.8 Contactless communication link and dual modes

One area of potential vulnerability for contactless technology is the radio frequency communication link. It may be possible to specifically enhance electromagnetic or power attacks as discussed in the previous chapter on smart card security. The attacker has an easier access to the field in which the card operates. He may disturb that field as he pleases. On the other hand, these side-channels may be much noisier than measuring the power directly through the contact card interface. Appropriate countermeasures have to be efficiently implemented on both types of cards.

One important aspect though is considering the separation between communication modes for dual mode cards. An attacker may potentially try to start a communication on the contact interface and after a few commands, switch over to the radio-frequency link. The card needs to have built-in countermeasures against this kind of scenario. Along the same lines, specific side-channel countermeasures for instance such as applying a current stabiliser right underneath the contact interface, need to be equivalently applied to both interfaces; otherwise for example current consumption may be measured on the second interface while the first is supposed to be protected against power attacks. Thus separation of modes is a crucial issue to be taken into account on dual mode cards.

5.9 Chipcard technology

Looking at the threats directly related to the chip on the card, we found that there is no major difference between a single mode contact and contactless card.

Invasive and non invasive hardware attacks will essentially apply the same way on both technologies. However, one specific case to be considered is the fault side-channel. Faults may be much more difficult to induce as the card is basically meant to operate in an unstable electromagnetic field and already has appropriate backup mechanisms. On the other hand, contactless technology requires the card to be operated via inducted current, thus activating the right sensors on the card, or implementing standard side-channel countermeasures requires much more computation time and computing power, which can become a bottleneck in this specific scenario. The trade-off between cost and security for contactless cards is somewhat specific and needs to be carefully studied in order to achieve the same security level as contact cards at the same price.

5.10 Cryptography

From an application point of view, the cryptography in the card has to be secure and well implemented. Standard secret key and public key algorithms should be used depending on the required security level. Contactless cards have a drawback in the sense that they require more power to achieve the same computation performance of cryptographic algorithms as contact cards. Crypto-coprocessors or even basic CPU operations are time and power consuming when it comes to complicated cryptographic algorithms. Thus, for equivalent security parameters, power supply needs to be increased or the communication range needs to be reduced in comparison with contact cards.

In that sense, one could argue that contactless technology is “less secure” than contact card technology; however this is just a matter of ratio between power supply requirements and security level. Then again, for typical contactless applications such as transport applications, the need for strong public key cryptography may be of limited relevance.

5.11 Conclusion

There are a number of potential threats that have to be studied carefully in contactless technology, be it on chip, or at the application level, but several means and countermeasures exist to provide secure solutions.

6 Comments on current threats in Protection Profiles

This part of the document examines how existing Common Criteria Protection Profiles concerning smartcards and smartcard applications are affected by specific issues related to the contactless interface (more specifically "proximity cards", as specified by ISO/IEC 14443).

6.1 Relevant protection profiles

From a list of protection profiles (see table 6), we selected some profiles most relevant to applications or devices which could exist in a contactless variant:

Table 4: Commented Protection Profiles

ID	*Protection Profile Name*	*Issuers*	*CC version*
PP/0103 SCSUG-SCPP	Smart Card Security User Group, Smart Card Protection Profile. Version 3.0	Mondex International, American Express, Europay International, JCB Co Ltd, MasterCard International, Visa International, NIST (USA), NSA (USA)	2.1
PP/9911	Smart Card Integrated Circuit with Embedded Software v2.0	EUROSMART: ATMEL Smart Card ICs, BULL - SC&T, DE LA RUE - Card Systems, GEMPLUS, GIESECKE & DEVRIENT GmbH, HITACHI Europe Ltd, INFINEON Technologies, MICROELECTRONICA Española, MOTOROLA - SPS, NEC Electronics, OBERTHUR Smart Card, DS, ORGA, PHILIPS Semiconductors, SCHLUMBERGER Cards Division, SCSSI, ST Microelectronics	2.0
PP/9903	Profil de Protection pour Carte à puce Billettique Avec et Sans Contact v1.2	RATP, SNCF	2.0
PP/9806	Smartcard Integrated Circuit Protection Profile v2.0	Motorola Semicomductors, Philips Semiconductors, Siemens AG Semiconductors, STMicroelectronics, Texas-Instruments Semiconductors	2.0

Sources:

- http://www.scssi.gouv.fr/fr/confiance/pp.html
- http://www.cesg.gov.uk/assurance/iacs/itsec/documents/protection-profiles/index.htm
- NIST

6.2 Contactless issues

Most of these documents would need some changes due to a transition to contactless (an exception is PP/9903 which already considers contactless).

In many cases, these changes are superficial, often it would be enough to include relevant contactless standards (such as ISO 14443) in the list of references

This is because Protection Profiles list *Information Technology Security* requirements in a given application, and the requirements are unchanged when met by different means (e.g. induction instead of contacts).

It is conformance to the profiles (Security Targets), rather than the profiles themselves, which needs to be most worked upon.

In only a few cases, these profiles detail threats, and these sections would need to be updated to account for contactless-specific threats, as discussed above.

The suggested modification for each profile are described in the following table:

Table 5: Proposed Modifications to relevant Protection Profiles

ID	***Proposed modifications***
PP/0103 SCSUG-SCPP	§1.4. Reference to ISO14443 needs to be updated. §2.1 should include the contactless interface description. §3.3.1.4. An item should be added to state that an attacker may exploit contact and contactless interactions (e.g. send commands in contactless and in contact mode). §3.3.1.6. and 3.3.1.7 the contactless interface should be added to T.I-Leak and T.Env-Strs list of interfaces §4.1. O.I_Leak The contactless link needs to be added. §4.2 O.E.Pwr_Clock: To be updated §5 An item should be added: “The TSF shall include the operating mode detection.” §6 The rationale must be subsequently updated. Annex A The glossary should include contactless terms Annex B Should be updated to include the contactless description Annex D Should be updated The following should be added to the threats and security objectives: Threat: Unauthorised use of contact-only functions when the TOE is used in contactless mode and vice-versa. (Security conditions may depend upon the operating mode). Objective: The TOE must be able to reliably indicate the contact / contactless chip operating mode.
PP/9911	§2.1 The “I/Os” could be described as Contact and Contactless. §3.3.4 The unauthorised modification of assets through a contactless communication hidden from the legitimate card holder. §4.2.5 An objective stating that the TOE that security conditions depending upon the operating mode (contact / contactless) are correctly enforced. §4.2.4 and 4.2.5 An objective stating that organisational measures must prevent covert contactless use of the TOE. §8 The rational must be subsequently updated. Annex A The glossary should include contactless terms
PP/9903	None, as it already describes contactless applications.
PP/9806	This document does not seem to need any modifications as it describes the chip manufacturing process.

Table 6: List of Protection Profiles

ID	*Protection Profile Name*	*Issuers*	*CC version*
PP/0103	Smart Card Security User Group, Smart Card Protection Profile (SCSUG-SCPP)	Mondex International, American Express, Europay International, JCB Co Ltd, MasterCard International, Visa International, National Institute of Standards and Technology (United States of America), National Security Agency (United States of America)	2.1
PP/0101	Intersector Electronic Purse and Purchase Device (version without last purchase cancellation) Version 1.3	SFPMEI	2.1
PP/0010	Smart Card IC with Multi-Application Secure Platform v2.0	Eurosmart	2.1
PP/0002	Transactional Smartcard reader v2.0	Cyber-COMM	2.1
PP/9911	Smart Card Integrated Circuit with Embedded Software v2.0	EuroSmart	2.0
PP/9909	Intersector Electronic Purse and Purchase Device v1.2	GIE Cartes Bancaires CB, Société Financière du PMEI	2.0
PP/9908	Intersector Electronic Purse and Purchase Device (Version for Pilot Schemes) v1.2	GIE Cartes Bancaires CB, Société Financière du PMEI	2.0
PP/9907	Automatic Cash Dispensers / Teller Machines	Bull, Dassault AT, Diebold, NCR, Siemens Nixdorf, Wang Global	2.0
PP/9906	Configurable Security Guard (CSG)	Délégation Générale pour l'Armement	2.0
PP/9905	Firewall à exigences élevées v2.2	Délégation Générale pour l'Armement	2.0
PP/9904	Firewall à exigences réduites v2.2	Délégation Générale pour l'Armement	2.0
PP/9903	Profil de Protection pour Carte à puce Billettique Avec et Sans Contact v1.2	RATP, SNCF	2.0
PP/9810	Smartcard embedded software v1.2	Schlumberger	2.0
PP/9806	Smartcard Integrated Circuit Protection Profile v2.0	Motorola Semicomductors, Philips Semiconductors, Siemens AG Semiconductors, STMicroelectronics, Texas-Instruments Semiconductors	2.0
PPnc/0102	CB-EMV Payment/Withdrawal Smart Card Application v. 0.40	Groupement des Cartes Bancaires "CB"	not certified
PPnc/0009	PP Smartcard Personalisation Sites with Mailer Handling	GIE Sésam-Vitale, GIP Carte de Professionnel de Santé	not certified
PPnc/0008	PP Smartcard Personalisation Sites without Mailer Handling	GIE Sésam-Vitale, GIP Carte de Professionnel de Santé	not certified
PPnc/0007	PP Smartcard Embedding Sites	AFPC	not certified
PPnc/0006	PP Autorité de Certification v2.6	SCSSI	not certified
PPnc/0005	PP Autorité d'Enregistrement v2.6	SCSSI	not certified

PPnc/0004	PP Infrastructure de Gestion de Clés v2.6	SCSSI	not certified
PPnc/0003	PP Ressource Cryptographique pour une Infrastructure de Gestion de Clés v2.6	SCSSI	not certified
PPnc/9804	Outils de sécurisation des messages v1.5	SCSSI	not certified
PPnc/9803	Transactions portant sur des données confidentielles	Ministère de l'Economie, des Finances et de l'Industrie	not certified
PPnc/9802	Transactions portant sur des données non confidentielles	Ministère de l'Economie, des Finances et de l'Industrie	not certified
PPnc/9705	Tierces parties de confiance v0.9	SCSSI	not certified

.

7 Conclusion

Throughout this document, we have investigated potential threats that may apply to contactless chipcard technology. We have listed several vulnerabilities and have discussed possible countermeasures.

In general, we have found contactless technology not to be intrinsically more vulnerable than contact cards for the majority of threats, including all threats related to the chip on the card. Potential security issues such as surreptitious card operation may arise from differences at the application level, but can mostly be solved through that same application. Issuers may have to rethink their application according to a contactless environment, but solutions and countermeasures to potential attacks exist in this environment the same way they do in the contact card application world.

Encryption and authentication mechanisms should be used whenever possible ; issuers should be aware of the potential vulnerability of the card against side-channel analysis and find the right balance between the risk associated to such attacks and the cost of appropriate protection mechanisms. The trade-off might differ between contact card technology and contactless technology.

From a certification point of view, relevant Protection Profiles have been discussed and suggestions have been made as to how they should be augmented in order to take into account the specificity of contactless products.

Some updates are strongly encouraged for instance on the Smart Card Protection Profile of the Smart Card Security User Group [PP/0103 SCSUG-SCPP] and on the Smart Card Integrated Circuit with Embedded Software Protection Profile [PP/9911]. The recommendations we make should be proposed to TB3, the eEurope Trailblazer involved in certification.

Issuers on their side should be aware that updated Protection Profiles can best serve their interest and are encouraged to make best usage of the available certification processes. The intended objective of this document is that it will contribute to stimulate involved actors to share their knowledge on and to increase their awareness of the specificity of contactless technology.

Annex A
(informative)

Bibliography

[1] I. Duthie and G. Waters, “Contactless smart cards: a dream or a need – limited or driven by technology?”, Card Forum International, Every Card Publisher Ltd., Volume 4 Number 4.

[2] B. Moreau, “Secure contactless microcontrollers – New opportunities for the public transport operators, the telephone companies and the banks”, Smart Card ’97 Convention Proceedings.

[3] Java Card Special Interest Group. *Smart Card Overview*.

http://www.javacard.org/others/smart_card.htm - Overview

[4] N. Knapich and J. Corcoran, “Challenges in contactless smart card manufacturing”, Card Forum International, Every Card Publisher Ltd., Volume 5 Number 4.

[5] M. Daroux, J. Nardi, X. Xing, G. Moutsios, J. Fang, T. Hadbavny and F. Shokoohi, “Thin Flat Batteries For Smart Card”, Cartes ’98 Conference Proceedings.

[6] D. Berger, *Contactless chipcards and standardisation (Part I).* Card Forum International, Every Card Publisher Ltd., Volume 3 Number 2.

[7] D. Berger. *Contactless chipcards and standardisation (Part II).* Card Forum International, Every Card Publisher Ltd., Volume 3 Number 3.

[8] D. Pratone. *ISO/IEC JTC1 SC17 activity related to IC Cards - 2001 activity report.* Doc. Code 2002.00152 25/01/2002

[9] W. Rankl and W. Effing, Smart Card Handbook, 2nd edition, New York, John Wiley & Sons, 2000.

[10] P. C. Kocher, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems”, in CRYPTO'96, Lecture Notes in Computer Science #1109, Springer Verlag, 1996.

[11] D. Boneh, R. DeMillo and R. Lipton, “On the Importance of Checking Cryptographic Protocols for Faults”, in EUROCRYPT’97, Lecture Notes in Computer Science #1233, Springer Verlag, 1997.

[12] J. Kelsey, B. Schneier, D. Wagner, C. Hall, “Side Channel Cryptanalysis of Product Ciphers”, in ESORICS'98, Lecture Notes in Computer Science #1485, Springer Verlag, 1998.

[13] P. Kocher, J. Jaffe, B. Jun, “Differential Power Analysis”, in CRYPTO'99, Lecture Notes in Computer Science #1666, Springer Verlag, 1999.

[14] L. Goubin, J. Patarin, “DES and Differential Power Analysis”, in CHES'99, Lecture Notes in Computer Science #1717, Springer Verlag, 1999.

[15] L. Goubin, J.-S. Coron, “On boolean and arithmetic masking against differential power analysis”, in CHES'00, Lecture Notes in Computer Science#1965, Springer Verlag, 2000.

[16] K. Gandolfi, C. Mourtel and F. Olivier, “Electromagnetic analysis : concrete results”, in CHES'01, Lecture Notes in Computer Science #2162, Springer Verlag, 2001.

[17] J.-J. Quisquater and D. Samyde, “ElectroMagnetic Analysis (EMA) Measures and Counter-Measures for Smart Cards”, in E-Smart Smartcard Programming and Security, Lecture Notes in Computer Science #2140, Springer Verlag, 2001.