

Security Aspects of Smart Cards

Authors:
Eugene Lockett
Sung Kyu Park
Guangcheng Jiang
Mike Riddle

Term Project CS574
Fall 2003
San Diego State University

Date Submitted: November 3rd 2003
Word Count: ~4600

Contents

1. INTRODUCTION	3
1.1. Historical Background	3
1.2. Overview	3
2. TECHNOLOGIES	4
2.1. Types of Smart Cards	4
2.2. Security-Related Standards	6
2.3. Physical Architecture	7
2.4. Security Features Available To Smart Cards	9
2.5. Operating Systems	9
3. APPLICATIONS	10
3.1. Telephone	10
3.2. Transportation	11
3.3. Computer Access Control	12
3.4. Banking	12
3.5. Health care	13
4. ETHICAL ISSUES	14
5. ATTACKS AND COUNTERMEASURES	16
5.1. Classifications of Attackers	17
5.2. Internal Attacks	18
5.3. External Attacks	19
6. CONCLUSION	21
REFERENCES	22

1. Introduction

In modern day society, cards have proven to be convenient tokens for identification and authentication in day-to-day activities. Most people carry a collection of such cards with them whenever they leave home, be it credit cards, identification cards, or perhaps a grocery store club card and a library card. They are small, convenient, and make certain information easily available. It makes sense that the progression of technology would involve extending the idea of having small convenient data-holding security items to the next level. Smart cards are this next level.

1.1 Historical Background

The smart card had its start in Japan back in 1970, when Japanese inventor Kunitaka Arimura patented the idea [Hend2001]. Further progress was made in the mid-seventies when Roland Moreno filed more patents, this time in France. While Kunitaka focused on technical aspects of the smart card, Moreno paid more attention to functional aspects of the card, such as protecting the memory on the card. These patents finally expired in 1996, allowing many more companies to work on developing the technology.

1.2 Overview

Basically, the smart card is a card with an integrated circuit embedded and some input/output ability, usually metal contacts. Depending on the type of smart card, the chip can be either straight memory, memory with some security logic, or a full microprocessor with memory. The function of a card can be as simple as merely storing some value, such as some dollar amount that gets decreased every time it is used. A card

can also be multi-functional, running a program that requires special authentication and cryptographic keys, for example. All cards have a common communication interface with a host (card reader), as described in ISO 7816. This standard defines the physical characteristics, such as dimensions of the card, thickness, flexibility, and dimensions of the contacts, as well as the specifications for electrical signals and protocol of communication with the card.

This document will cover some of the important security applications of smartcards, as well as technologies involved in the smart card. In any security system, there are threats and controls, and later will be discussed some of those pertaining to smart card security. Finally, when storing personal information on a card, there arise certain ethical issues, and such will be discussed in this document as well.

2. Smart Card Technology

2.1 Types of Smart Cards

The technologies that are used in smart cards are widespread. The three main categories of smart cards used are contact cards, contactless cards, and dual interface cards (combicards). Contact cards are inserted directly into a smart card reader. The reader makes physical contact with the contact pads on the smart card to communicate with the card and provide power to it. The contact smart card is more secure compared to the contactless one, because it very difficult to “listen in” on communications between the card and reader, due to the direct contact the two make. Contactless cards use radio frequencies to communicate that are susceptible to interception.

Contactless card readers use radio frequencies to power and communicate with the card. Depending on the sensitivity of the card's radio antenna, the card's orientation to the reader, and other environmental conditions, the contactless card can have an access range of 2 centimeters to 1 meter away from the reader [SCA2002]. A user does not have to be extremely close to the reader in order to be granted access making the contactless card a convenient tool when allowing access to secure locations. The ICC (integrated circuit chip) on the smart card is sealed beneath the surface of the card. With this sealed architecture, the card is resistant to damage from the outside environment, such as dust and moisture. Another advantage is that there are no mechanical parts to be maintained on the card readers. Dual Interface cards, or combicards, are a combination of the contact and the contactless cards. Both types are integrated into one card to allow the card to be used with both types of readers.

For all three types of smart cards, there are three levels of chip complexity: memory, wired logic, and microcontroller unit (MCU) cards [Drei1998]. Memory cards generally store authentication information to be exchanged with a card reader. The more secure cards are also able to protect parts of memory from unauthorized writing. Wired logic cards use a special circuit to authenticate to readers. It is able to use encrypted communication to verify that the reader can be trusted. Since it is hard-wired, it is not modifiable after being manufactured. A MCU card, the most complex of the three, has access to encryption methods available in software or hardware. Other features include biometric verification, tamper-resistant memory contents, and digital signatures.

2.2 Security-Related Standards

ISO 14443 and ISO 15693 are two important standards that describe two different types of contactless cards. Both standards operate at the 13.56 Mhz frequency range. ISO 14443 defines proximity smart cards, which operate within a four- inch range of a smart card reader [SCA2002]. The closer the smart card to the reader, the more power that can be sent to the card via the RF signals being used. This power allows the smart card to be equipped with a microprocessor and a cryptographic coprocessor. ISO 14443 cards are able to transfer data at a rate of 106 Kbps and store up to 64 Kbytes of data on the card [SCA2002].

With a cryptographic coprocessor, there are a number of encryption methods available for use: triple DES, AES, RSA, and elliptical curve cryptography (ECC). Due to the fact that the card must be very close to the reader to communicate, it is hard for someone to try to access someone else's card without him/her becoming aware of it. These security features allow ISO 14443 cards to be used in electronic cash applications. The ISO 15693 cards are designed to operate at a farther range of 3 feet. The increased range lowers the amount of power that can be sent to the smart card. This limitation causes a simpler design to be implemented on the card, which would require less power. These cards can be either simple memory cards or wired logic smart cards. Some encryption methods available are DES and triple DES. ISO 15693 cards have a data transfer rate of 26.6 Kbps and a storage capacity of 2 Kbytes [SCA2002]. This card is better suited to access control applications, where a better range is a good trade-off with simpler and slower card transactions. The following is a table of the more common smart card-related standards.

ISO #	Description
ISO 7816-1	Physical characteristics of contact cards
ISO 7816-2	Dimensions and location of the contacts
ISO 7816-3	Electronic signals and transmission protocols of contact cards
ISO 7816-4	Industry commands for interchange of contact cards
ISO 7816-5	Number system and registration procedure for application identifiers of contact cards
ISO 7816-6	Interindustry data elements of contact cards
ISO 14443	RFID cards; contactless proximity cards operating at 13.56 MHz in up to 5 inches distance
ISO 15693	RFID cards; contactless vicinity cards operating at 13.56 MHz in up to 50 inches distance

Table 1. ISO Standards for Smart Cards [www.iso.org & www.smartcardalliance.org]

2.3 Physical Architecture

Despite its small size, a smart card contains almost all the components of a full size computer system. These components consist of I/O control, a CPU, and various kinds of memory. The memory used can be divided into three types: ROM, RAM, and non-volatile memory (NVM). ROM is memory that has its contents written only once- when

the card is manufactured. This is where the card's operating system resides. RAM is where the card's applications are run when power is supplied to the card. Without power, all of the RAM's contents are lost; therefore any data that needs to persist on a smart card cannot be stored in RAM. This problem is solved by using NVM to provide an area of memory to permanently store data. The most common type of NVM used is EEPROM, which allows variable data to be stored long term. However, there is a limit to the number of times that you can modify the contents of the EEPROM, usually around 100,000 times [Jurg2002]. Security is increased by integrating the CPU and memory onto one chip, making it very difficult to try to see the communication that occurs between the two, without the use of special probing devices.

Using the concept of "least privilege", memory on a smart card is categorized into three zones with different access levels [Zore1994]. The three zones are the Manufacturer's zone, the Secret zone, and the Status zone. The Manufacturer's zone stores data such as the card ID number, and is only written to during the manufacturing process. Only the CPU is allowed access to this zone. The Secret zone holds information including the user's PIN and the issuer's key. This zone provides read/write access to the CPU, the card issuer, and the user, as long as these entities are authenticated with some sort of key. The third zone is the Status zone, which is the area of memory that keeps track of attempts to access the card. After a certain number of failed access attempts, a card can lock itself from the user or can destroy the data on the card, to prevent unauthorized access. This zone is used for auditing purposes, so it is only accessible to the CPU and the card issuer with the appropriate key. Only these entities should be allowed to see the user's audit trail.

2.4 Security Features Available To Smart Cards

As smart cards are used more as a substitute for cash, it becomes more important that the card and the card reader can authenticate each other. There are a variety of security features available that allow this to be done. Among the standard methods that can be used are DES, AES, RSA, and ECC. Another specification called Cryptoki, or PKCS-11, is used to provide authentication services, such as key management/ generation in public key encryption [Jurg2002]. This same specification is also used with Netscape for authenticating transactions on the Internet.

2.5 Operating Systems Used

The three main operating systems commonly used on smart cards are Java, Windows, and Multos [Jurg2002]. All three are stripped-down versions of their PC counterparts. Java cards have a security manager that authorizes whether applets are allowed to run on the card. The Multos card runs byte code assembly language for its applications. It creates a firewall between applications so that if an application goes astray, it will cause the least amount of damage possible. The Windows cards have a FAT file system that uses access control lists to prevent unauthorized access to application and data files. However, Microsoft is no longer supporting its Windows for smart cards.

3. Applications

Smart cards are already being used extensively in Japan and Europe and are gaining popularity in the U.S. Smart cards are currently used in telecommunications, transportation, computer networks, e-commerce, banking, personnel identification, and the health care industry.

3.1 Telephone

Public telephones using cash have some limitations:

- The payphone must be very durable to protect the cash from theft.
- The revenue must be physically collected.
- The payphone can become full, jammed or vandalized.

Smart cards are one of the solutions to overcome these problems. They must be able to operate reliably in a wide range of environmental conditions, and must be easy to handle for all types of users, and they must be relatively expensive to counterfeit when compared to the maximum value on the card. Even though magnetic and optical cards have been used with success over the years, most payphone operators have opted for smart cards as the most effective card form [Hend2001].

The first generation of smart telephone cards was made up of simple memory cards. These cards contained an issuer identification area, logic that prevented the value of the card from being increased without authorization, and usually a relatively small maximum account value. The second generation had higher maximum counts, card

authentication mechanisms that protected against counterfeiting and emulation, and logic that protected the card in case it is removed during a transaction. Next generation cards use a dynamic challenge and response authentication method, which makes counterfeiting virtually impossible, along with a user memory area. With the aid of public key encryption, different companies' smart cards can be used at the same telephone booth. Each telephone company issues smart cards using its own set of private keys, and the telephone booths store the public keys of several card issuers, allowing different companies' cards to be used with the same booth.

3.2 Transportation

An efficient public transportation service requires seamless transition between many different transit services, allowing passengers to travel on a single ticket across several operators' services. It may also be necessary to have some agreement with a national or local railroad operator if it provides complementary services. All of these systems bring with them the need to divide revenue between operators fairly [McDo2000].

Magnetic-stripe cards have been used as tickets on all forms of public transportation for many years. However, they have several drawbacks. They give little management information, and higher value tickets, such as annual season passes, are a target for fraud or theft. Smart cards provide for the collection of usage data and allow more accurate tracking of revenue.

Smart cards in transportation systems provide many benefits. Eliminating the need for cash collection improves security for the transit drivers, since there is no cash onboard. Time efficiency is also increased because there is no delay associated with

drivers verifying or selling tickets.

3.3 Computer Access Control

Most computers are accessed by a combination of user id and password. Valid passwords can be obtained by looking over people's shoulders or by leaving sticky notes on the computer. Passwords can be also stolen by monitoring data traffic, or in some cases, by hacking into system files [Hend2001].

A more secure form of control involves the use of an intelligent token, such as a smart card. Smart card readers are becoming easily available for personal computers, and this is one of easiest forms of tokens to implement. The password is checked by the card and need not be stored anywhere on the system. User id can be provided either by the card or the user. The card may contain a user profile, including preferences and group permissions where access to specific system functions is specified.

The card can also store a range of passwords and authentication mechanisms. The user authenticates himself or herself to the card once, and then has no need to remember the dozens of passwords which he or she may need to cross firewalls, access different websites, authorize payments, and so forth.

3.4 Banking

Nearly all debit, credit, and charge cards work within the framework of a card association, where merchants agree to accept cards from all issuers within the association. The need to maintain backwards compatibility is one of the biggest limitations on the speed of technology diffusion in the card schemes [Hend2001].

One of benefits of the smart card is that it allows people to use it as the electronic purse. While credit cards offer 'pay later' and debit cards are 'pay now', electronic purses are prepaid.

We can also see electronic passbooks, for accounts that traditionally have been maintained using printed records in a book. Most passbooks carry a magnetic stripe, which duplicates all or some of the printed data in the book, but these suffer from security weakness. The use of smart cards will allow the book to be used as a more secure identification of the account holder.

Banks are able to hold more customer data on smart cards held by the customers. This allows them to offer an increased range of services at remote locations where full on-line access would be slow or unfeasible. They can also reduce operating costs, and generate new revenue streams, and build market share, through new distribution channels.

3.5 Health care

The dominant motive for introducing health cards is control of costs. They can verify if the person claiming medical services is insured, and to correlate claims for payment with both individual patient records and the doctor's accounts. These simple health cards have limitations.

One of benefits from smart health cards is that whenever your clients are transported to the emergency room or to their Doctor's office, the Health Smart Card will contain all of the health and insurance information needed by the health care provider. It might be read in a participating ambulance, emergency department, or doctor's office.

If the patient is unable to answer the health care provider's questions for whatever reason then, with the smart card, detailed information is still available. If the patient is unable to answer the health care provider's questions for whatever reason then, with the smart card, detailed information is still available. This may be life saving such as in instances of diabetic coma. You could offer the Health Smart Card at your expense to your prospective clients as an incentive to engage your services. This would then be a marketing tool to sell your services.

If medical records involve large quantities of data, it may not be economic with current smart card technology to store the whole record on the card. In this case, we can store the data in an on-line system, using the card to control access to the records. The card keeps only essential summary information.

4. Ethical Issues

By itself, a smartcard is just a little piece of technology that executes encoded instructions when voltage is applied to the “Vcc” contact. It reads and stores data, manipulates bits, makes computations, and changes voltage on the i/o port. From this perspective it wouldn't seem that there's much to talk about in a section entitled "Ethical issues" in reference to the smartcard. Of course, such is true with any technology; from a purely technical description of a device there tends not to arise many ethical issues. The *application* of a technology is where ethical issues arise. Certain applications of smartcard technology give way to potential issues, namely applications involving the storage of personal information.

One such application, which is full of nothing but good intentions, was mentioned in an article in the Omaha World Herald [Jord2003]:

You're driving alone one night when WHAM! a car broadsides you, knocking you unconscious.

In the rescue squad, an attendant finds your universal health card and slips it into a hand-held computer, which quickly displays your name, blood type, allergies and other vital information.

At the hospital, a nurse in the emergency room punches up more information in the computer: your doctor's name; a family member to contact; a list of medications you take; operations you've had; cautionary comments from your doctor.

The idea of the "Health Data Card" system is to have one smartcard in every person's pocket and a card reader at every hospital and in every ambulance. Then, in the case of an emergency, the smartcard will be able to provide a great deal of information to emergency personnel in a short period of time, even if the patient is totally incapacitated. This sounds appealing, but the implications of having all of this very personal information on a single card must be considered.

First of all, the integrity of the data on the card is priority. If doctors will be making medical decisions based on the bits of data stored in the EEPROM of a smartcard, then there must be no question as to the integrity of that data. Due to the nature of the information, the card will no doubt need to be updated periodically. This means a great deal of effort on the part of the developers must be devoted to making sure

that card can be written to only by authorized sources, necessitating very secure authentication with anyone trying to read it. Users of the system will need to trust that such security has been reliably implemented.

Secondly, one must consider how this technology can be potentially misused; how might someone benefit from stealing or somehow otherwise obtaining the data on the card? Such data could take identity theft to another level, giving the thief the allergies and prescriptions of the victim. Additionally, with malicious intent, the information could be potentially misused to cause harm to another. Therefore, secure authentication is also needed in allowing the data to be read, and the users of the system will have to trust that such security implemented is dependable.

5. Attacks and Countermeasures

The effectiveness of smart cards in delivering security is one of the reasons that they have been so widely adopted, especially in financial services and mobile phones. As in any field, security standards do not stand still. There will always be those who seek to break security shields for fraudulent, ethical or experimental reasons. Indeed, smart cards can be vulnerable to attacks internally or externally [Henr2001]. Internal attacks involve performing operations directly on the chip embedded inside the smart card. External attacks involve operations from outside, through its normal contacts on contact cards or through radio interface on contactless cards. Two recently reported attacks involved the differential power analysis for extracting data from semiconductor [Sanl2002] and partitioning technique for cloning GSM cards [Rao2002].

In this section, we will briefly describe some examples of internal and external attacks on smart cards as well as the corresponding countermeasures against those attacks.

5.1 Classifications of Attackers

When evaluating the level of tamper resistance (security) offered by a given product it is important to know what level of attack it can or cannot stand. According to Abraham, et al. at IBM [Abra1991], the attackers are grouped into three classes, in ascending order, depending on their abilities and attack strengths.

Class I (Clever Outsiders):

They are often very intelligent but may have insufficient knowledge of the system.

They may have access to only moderately sophisticated equipment. They often try to take advantage of an existing weakness in the system, rather than try to create one.

Class II (Knowledgeable Insiders):

They have substantial specialized technical education and experience. They have varying degrees of understanding of parts of the system but potential access to most of it. They often have highly sophisticated tools and instruments for analysis.

Class III (Funded Organizations):

They are able to assemble teams of specialists with related and complementary skills backed by great funding resources. They are capable of in-depth analysis of the system, designing sophisticated attacks, and using the most advanced analysis tools. They may use Class II adversaries as part of the attack team.

5.2 Internal Attacks

Internal attacks are invasive physical attacks that require removal of the microprocessor from the card. This is normally done by using a sharp knife to cut away the plastic behind the processor until the epoxy resin becomes visible. The resin is then removed by fuming nitric acid followed by acetone wash. Once the silicon surface is exposed, it may be analyzed by a light or electron microscope, probed using needles, or modified using a focused ion-beam (FIB) system. To prevent the data from being altered during the successive operations, the capacitor network that generates the E2PROM programming voltage, may be destroyed with lasers, ultrasonic beams or focused ion beams [Ande1996].

It should be pointed out that most of the internal attacks are Class III attacks. These attacks are aimed at enabling manufactures and designer to identify vulnerable elements of their systems and to enhance the security.

Microscopic Analysis

In this attack, light and electron microscopes are employed to inspect the physical structure of the chip. This could permit the analysis or reverse engineering of the device [Blyt1993], or of specific areas such as security mechanisms or data storage.

Countermeasures: bus scrambling, address scrambling, anti-etching layers, and a metalization layer over the whole chip. Some high-security chips include circuits that detect the radiation of an electron microscope.

Mechanical Probing

In this attack, the analyst uses very sharp needles (mechanical probes) [Ande1996] to make galvanic contact with metal tracks on the exposed chip. The data transported over the buses of a device in real time operation can be trapped under a risk of damaging the chip.

Countermeasures: 0.5 μ or smaller feature size and a metalization layer over the whole chip.

Use of Test Modes

During manufacturing of smart cards, test modes and test contacts on the chip are employed for testing. They are disabled by software and/or hardware upon successful completion of the tests. Unfortunately, these features sometimes can be located, reestablished, and misused to retrieve secrets from the card.

Countermeasures: anti-etching layers.

5.3 External Attacks

External attacks (semi- or non-invasive attacks) involve the use of a card – often a large number of cards. The attack can be designed using an old or invalid card, then carried out on a live card. Non-invasive attacks such as power analysis require only a moderate

capital investment, plus a moderate investment of effort in designing an attack on a particular type of device. This makes this class of attacks particularly attractive although the chance of success is low due to the expense time.

Circuit Analysis

Circuit analysis is a non-invasive attack and involves low-frequency manipulation of the inputs and observation of the outputs [Ande1996]. For example, a short voltage drop on DS5000 security processor can release the security lock without erasing the secret data sometimes. Low voltage can facilitate other attacks. One card has an on-board analog random number generator, used to create cryptographic keys, which will produce an output of almost all 1's when the supply voltage is lowered slightly.

Countermeasures: detection circuits on chips and on-board clock generation.

Measurement of Operating Parameters

In this semi-invasive attack where the chip is exposed, attackers try to read data directly from the memory of smart cards. This is done by measurement of parameters including the current or the operation time of the chip on certain tasks, followed by deductions and analysis of the measured results. One particular successful attack is *differential power analysis* (DPA) discovered by Kocher, et al [Koch1999]. DPA measures the variations in power used by the chip as it performs arithmetic, and analyzes these variations to extract cryptographic keys and other data.

Countermeasures: null operations, random variations within a single operation, data making [Mess2002], and randomized power masking [Beni2003].

Induction of Errors

In this attack, secret data (particularly the secret keys) is extracted by deliberately inducing errors in the computation followed by deduction of the information. One widely known technique for inducing such errors is glitching – introduction of voltage transients into the power to the CPU on the target chip.

Countermeasures: detectors on chip and terminal authentication.

6. Conclusion

The future of smart cards will provide greater security and functionality. Even though there are quite a number of attacks that can occur on smart cards, the smart card technology is still secure. This holds true because the attacks that seriously threaten smart cards require highly sophisticated and expensive equipment in order to break into the card. Future smart cards will have a human interface, such as a screen and keypad embedded on the card, to allow a user to verify that a smart card terminal is not being spoofed [Jerg2002]. The screen would warn the user of an unauthorized or fake terminal. If improvements are made to the power sources for contactless cards, it is possible that Bluetooth technology could be used. This would allow much higher data transfer rates on the cards. Cards of the future will come even closer to functioning as regular PC's, with network access and multiple applications running on them. These “smarter” cards will be used so often in our daily lives, that we won't give a second thought to having a fully functional computer sitting in our wallet.

References:

- [Abra1991] Abraham, D.G., Dolan, G.M., Double, G.P., and Stevens, J.V. "Transaction Security System", *IBM Systems Journal*, 30:2, 206-229, **1991**.
- [Ande1996] Anderson, R., and Kuhn, M. "Tamper Resistance - A Cautionary Note," *Proceedings of Second Workshop in Electronic Commerce*, USENIX Association, Oakland, CA, **1996**.
- [Beni2003] Benini, L., Macii, A., Macii, E., Omerbegovic, E., Poncino, M., and Pro, F. "Energy-Aware Design Techniques for Differential Power Analysis Protection", *Proceedings of the 40th Conference on Design Automation*, June 2-6, **2003**, Anaheim, California.
- [Blyt1993] Blythe, S., Fraboni, B., Lall, S., Ahmed, H., and de Riu, U. "Layout Reconstruction of Complex Silicon Chips," *IEEE Journal of Solid-State Circuits*, 28:2, 138-145, **1993**.
- [Drei1998] Dreifus, H. and Monk, J.T. Smart Cards: A guide to building and managing smart card applications. New York: John Wiley & Sons, **1998**.
- [Hend2001] Hendry, M. Smart Card Security and Applications. Artech House, **2001**.
- [Jord2003] Jordan, S. "Smart Cards Can Store Key Medical Info Partners Envision Universal System Universal Health Card," *Omaha World - Herald*, Omaha, Neb, **2003**.
- [Jurg2002] Jurgensen, T.M. and Guthery, S.B. Smart Cards: The Developer's Toolkit. Upper Saddle River, NJ: Prentice Hall PTR, **2002**.
- [Koch1999] Kocher, P., Jaffe, J., and Jun, B. "Differential Power Analysis," *Proc. Advances in Cryptology (CRYPTO '99)*, 388-397, **1999**.
- [McDo2000] McDonald, N. "Multipurpose Smart Cards in Transportation: Benefits and Barriers to Use," December 8, **2000**. URL: <http://www.uctc.net/mainstream/papers/SmartCard.pdf>
- [Mess2002] Messerges, T.S., Dabbish, E.A., and Sloan, R.H. "Examining Smart-Card Security under the Threat of Power Analysis Attacks," *IEEE Transactions On Computers*, 51:5, 541-552, **2002**.
- [Rao2002] Rao, J.R., Rohatgi, P.R., and Scherzer, H. "Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards," *2002 IEEE Symposium on Security and Privacy*, May 12-15, **2002**, Berkeley, California.

- [Sanl2002] Sanlyde, D., Skorobogatov, S., Anderson, R., and Quisquater, J.-J. "On a New Way to Read Data from Memory," *Proc. First International IEEE Security in Storage Workshop*, December 11, **2002**, Greenbelt Marriott, Maryland, USA.
- [SCA2002] "Contactless Technology for Secure Physical Access: Technology and Standards Choices," Smart Card Alliance. 20 October **2002**. URL: http://www.datacard.com/downloads/ViewDownload.dyn?elementId=/repositories/downloads/xml/SC_Contactless_Whitepaper_030304.xml&repositoryName=downloads.
- [Zore1994] Zoreda, J.L. and Otón, J.M. Smart Cards. Boston: Artech House, **1994**