A Smart Card Based Student Card System

By

Hendrik Jacobus Bothma

DISSERTATION

Submitted in the fulfilment of the requirements for the degree

MASTER OF SCIENCE

In

INFORMATION TECHNOLOGY

In the

FACULTY OF SCIENCE

At the

UNIVERSITY OF JOHANNESBURG

SUPERVISOR: PROF S.H. VON SOLMS

November 2007

Abstract

A Smart Card looks like a normal plastic card that we use every day, but its capabilities and advantages are huge. Inside the card there is a small microprocessor capable of doing operations on data. With memory available on the card, data can be stored in a safe and secure location. This card can be used for various applications and is a big improvement on all of its predecessors. These applications can be anything from SIM cards in a cell phone to credit cards and cards used for access control. The Smart Card offers us better security and offline identification because of its own embedded microprocessor. The combination of Smart Cards with biometrics for security reasons will be a logical step and the ideal way to identify the person as the true owner of the card. This dissertation will investigate the use of contact Smart Cards in the University environment, more specifically as a University student card. The Smart Card will be combined with a fingerprint to enforce better security. The main purpose is to use the Smart Card and the biometric property for access control at various places on campus.

Table of Contents

List of Figures

Chapter 1: Overview

1.1 Introduction

A Student card is the main form of identification for access control on a University campus. At the University of Johannesburg the students and University personnel need the card to get in at the University gates, for access at the library and to print documents at the printing stations. Students living in University hostels or residences also need the card to get into their residence.

When a student writes a test or exam the student card must be present for “manual authentication”. A lecturer or assistant will walk through the exam venue and check everybody’s student cards.

Until the end of 2004, the University used magnetic stripe cards with a photo printed on the front, they then decided to change over to **RFID** (Radio Frequency Identification) cards, and these cards are currently still in use (at the time this dissertation was written, 2007). With the RFID card it is at least quicker to get access to the University. No direct line of sight is needed. The student can leave the student card in his wallet. That was one of the problems with the magnetic stripe card, the fact that the user needs to swipe the card.

But the **biggest problem** with both these technologies is that a person can give his card to someone else to gain access to the University. Or worse, the card can be stolen and there is no way the University will know who the right owner is and stop the other person from getting access to the University grounds.

A similar problem exists at the **exam venues**. A registered student for a subject can pay someone else to go and write the exam for him. There is no way to make absolutely sure that only the right people can gain access to the exam. All methods used at exam/test venues to check student cards are manual. It is easy to bypass the “system” and to write the test or exam for someone else, especially in very large rooms with many students.

1.2 Problem Statement

The problem is when using magnetic stripe cards and RFID cards there are no way to positively identify the presenter of the card as the true owner.

1.3 Solution

The solution that we will explore is to use Smart Cards combined with biometrics to truly identify the person presenting the student card. This way we use something the user has and something the user is to improve the security. When the Smart Card is inserted, the student’s fingerprint will be asked and then compared to the fingerprint template that is stored on the Smart Card. A Smart Card is the only card that can store the template of a biometric on the card. This allows for offline identification.

1.4 Objectives

The main objective will be to see if we can enforce better security and student identification using the Smart Card and fingerprint identification. We only want to allow access onto the campus to registered students with the correct card. A student that borrowed a card should not be allowed onto the campus.

The student card will be used for access control at the University gates, at the library, at residence entrances and exam venue doors. Other options for use of the card is for controlling the use of computer stations at the University’s computer labs, and the card can also be used as an e-wallet at the on campus student centre.

1.5 Deliverables

There will be three deliverables: this dissertation, a prototype system called Smart Card VeriSys and a comprehensive set of test results, using the Smart Card VeriSys to test the accuracy of the technology used in the prototype.

1.5.1 The Dissertation

This dissertation will discuss several factors ranging from Smart Cards, previous student cards to fingerprint matching. More information about encryption algorithms and Message Authentication Codes (MAC) used in this prototype, are available in the appendixes. This will be all the theory that is related to the project. Then we will take a look at the Smart Card VeriSys and its workings. This will include all the hardware and software used, tests done on the system and a user manual.

1.5.2 Smart Card VeriSys

The Smart Card VeriSys will be a working prototype illustrating the use of Smart Cards combined with biometrics for access control. A Smart Card reader with a fingerprint scanner will be used. The Smart Card VeriSys will also contain a database with all the registered students (this will be a test database and will not contain information of actual students). Ten Smart Cards will be used to test the system. The Smart Card reader and Smart Cards are ACS (Advanced Card Systems) products (see [6]).

1.5.3 Test Results

A wide variety of tests were done on the Smart Card VeriSys. These tests range from False Acceptance Rate and False Rejection Rate to User Throughput Rates for the prototype. All the results of the tests will be provided and discussed in chapter 9.

1.6 Approach

The approach followed for this dissertation was to start with a literature study. The first part of the literature study was on Smart Cards, examining their potential and current uses. The next step was to study previous systems used at the University to discover their flaws in an effort to improve the Smart Card system.

A literature study was also done on fingerprints, encryption algorithms and message authentication algorithms as this forms part of the Smart Card VeriSys system being built.

While building the Smart Card VeriSys system, the first objective was to communicate with the Smart Card, store data on the card and access it again.

The next objective was to communicate with the fingerprint scanner, to scan a fingerprint and store the fingerprint template on the Smart Card for verification.

The last step is to put the Smart Card VeriSys system through several tests and specifically the throughput test. This is to assess the system's performance.

1.7 Overview of the Document

The next 5 chapters (chapters 2 – 6) will be a literature study on some aspects related to the project. This includes technologies that will be used, technologies that were previously used and also the fingerprint matching algorithms that will be used in the dissertation.

1.7.1 Chapter 2: Smart Cards

We will take a look at Smart Cards, their capabilities and some of their advantages and disadvantages compared to other card types. We will take a look at the different components that a Smart Card is made of and how they function together, and then we will discuss the different standards that Smart Cards must conform to.

1.7.2 Chapter 3: Typical Student Card Types

This chapter will be about previous card types that the University used. We will look at how these cards function, and why they are now inferior to the Smart Card. Types of cards that will be discussed are magnetic stripe cards and RFID cards.

1.7.3 Chapter 4: Other Smart Card Applications

We will take a look at other uses of Smart Cards. There are a range of applications where Smart Cards are used and can be used. The functionality differs quite a lot from access control to financial services and phone cards. We will discuss the functionality of each application and the use of the Smart Card in that environment.

1.7.4 Chapter 5: Evaluation of Smart Card Applications

We will evaluate the applications of chapter 4 and see whether there are any short comings. Smart Cards might be the best card technology available today, but that doesn’t mean all the problems are solved. It is necessary to take a look at the impact of Smart Cards on the applications where they were used.

1.7.5 Chapter 6: Biometrics: Fingerprint

This will be the last general chapter of the literature study. Chapter 6 will be about fingerprint matching algorithms, how it is done and problems that can arise with fingerprints. We will look at possible attacks that can be performed on biometric access control systems.

From this chapter onwards every chapter will be specific to the Smart Card VeriSys. We start with an overview of Chapter 7.

1.7.6 Chapter 7: Smart Card VeriSys: A High Level Description

This chapter will discuss what will be done in the Smart Card VeriSys prototype. We will look at the authentication and registration processes. More information about the Smart Card will be given.

1.7.7 Chapter 8: Hardware Used for the Smart Card VeriSys

Chapter 8 will focus on hardware that is used in the Smart Card VeriSys prototype. This includes the Smart Card reader, Smart Cards and the computer.

1.7.8 Chapter 9: Testing the Smart Card VeriSys

Methods for testing the Smart Card VeriSys system will be discussed. The results of these tests will be provided and compared against each other.

1.7.9 Chapter 10: User Manual

The user manual will explain how to use the system. This will help users to understand the whole system and the functions it offers.

1.7.10 Chapter 11: Evaluation of the Results

Chapter 11 will be an evaluation of whether a Smart Card with a fingerprint scanner will work in the University environment, and whether the contact Smart Card is the best type of Smart Card to use for access control.

1.7.11 Appendix A: DES

This section will take an in depth look at DES and how the encryption algorithm works.

1.7.12 Appendix B: Triple DES

The functioning of Triple DES and various key options will be discussed in this appendix.

1.7.13 Appendix C: MAC

We take a look at mutual authentication codes and how they are used to gain integrity in a system.

1.7.14 References

This is the list of the references used for this dissertation, and includes articles published and web references.

As mentioned earlier, Chapter 2 is about Smart Cards. This is the main topic of the dissertation and it will be discussed first.

Chapter 2: Smart Cards

2.1 Introduction

Smart Cards are the future of card technology. This is a card that has its own microprocessor that can do operations on data, alter the data and store it on the card. This provides us with a lot of opportunities for application development (see [1]).

In this chapter we will take a look at characteristics of Smart Cards. We will see what makes them better and more useful than other card types. Next we will look at the components that they consist of and also the standards that they are regulated by.

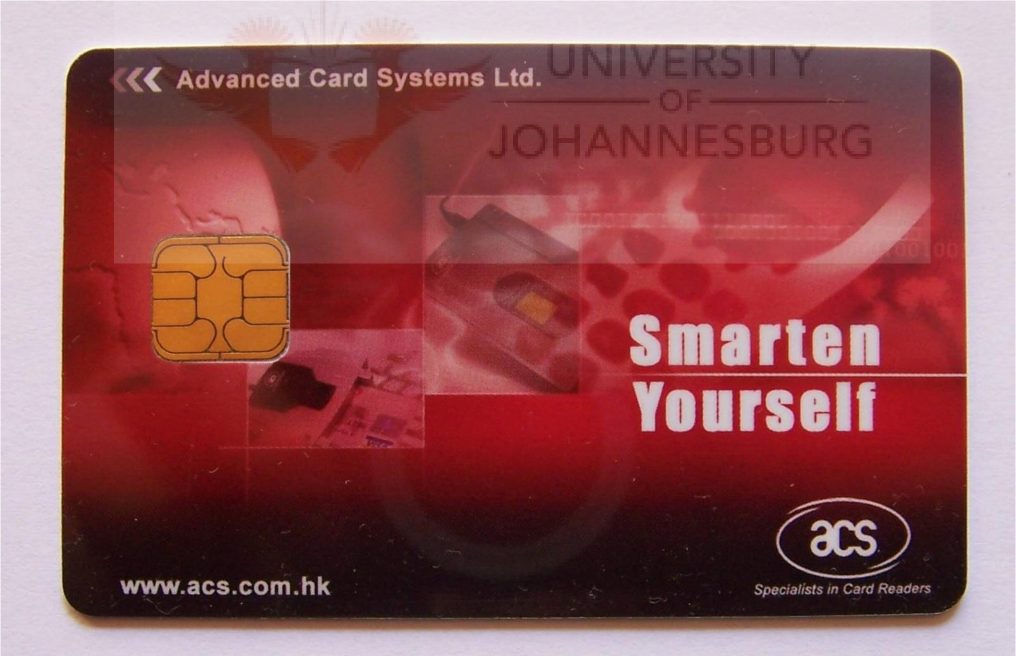


Figure 2.1: Advanced Card Systems Smart Card

A positive thing about Smart Cards is that they can only improve with time, but how much they can and will improve is still debatable. At the moment Smart Cards are not only improving in processing and data storage capabilities (which will be discussed later in the chapter). They are also improving on the interfaces that they use which will make them more user friendly and open them up for use in a bigger variety of applications.

2.2 Characteristics of Smart Cards

At the moment there are basically 4 different Smart Card types available for use, each one differing in interface and their capabilities.

2.2.1 Types of Smart Cards

The 4 options are: Contact, contact less, hybrid and combination cards (see [34]). We will start by looking at contact Smart Cards (see [10]).

2.2.1.1 Contact Smart Card

These cards need to be inserted into a card reader. It has a small gold plated chip interface which makes contact with the reader. These cards are exposed to a lot of contact that will shorten the card's life time because of wear and tear. The Smart Card gets its power through the contact pins of the reader to power up the processor on the card. The data that is communicated between the card and the reader travels through these pins (see Figure 2.1).

The second type of Smart Card that we will look at is the contact less Smart Card (see [10]).

2.2.1.2 Contact Less Smart Card

They use the same technology as RFID - that is radio frequency to communicate with the reader. These cards have a longer life time since no contact is needed. These cards, as with RFID, do not need a direct line of sight to work. The signal can be read through several materials. The Smart Card draws energy from the radio frequency (RF) that is emitted from the reader to do the operations (see [3]). All the data between the card and the reader are communicated using radio frequency.

The third option in different Smart Card types is hybrid cards (see [10]).

2.2.1.3 Hybrid Smart Card

These cards have two interfaces: contact and contact less. This sounds like the ideal solution. The only problem is that the two interfaces are not connected and can't share their data. This poses a big problem for certain applications, but there may be applications that will work better this way.

For instance in a card that is used as a multi application card, the one interface can be used for an application and the other interface can be used for the other application. The card can be used as a credit card (contact interface) and for access control (contact less interface).

The ideal solution for Smart Cards and applications would be a card that has both interfaces (contact and contact less). They will be able to share the data between the two interfaces. That’s where the next card comes in.

The last of the four types of Smart Cards is the combination card (see [34]).

2.2.1.4 Combination Smart Card

The latest Smart Card to arrive is the combination card. This card has only one interface, but it is a combination of contact and contact less interfaces. Thus it can be used on both contact and contact less card readers. The data is accessed through one interface and can thus be used by any one of the two reader types. This type of Smart Card is perfect for a multi application card or just about any other application where Smart Cards are used.

Now that we have discussed the types of Smart Cards that are available, we will take a look at some aspects of Smart Cards. The first point that we should mention about Smart Cards is the security mechanisms that the card have.

2.2.2 Strong Security

Smart Cards enforce strong security and can be used with a pin or a biometric for authentication. The strongest security would be to use the card combined with a pin and the biometric, but that would be time consuming, especially with access control (see [4]). This project will use biometrics, more specifically fingerprints combined with the Smart Card. The fingerprint template is stored on the Smart Card and the presented fingerprint is then matched to the stored template. This also allows for offline identification.

When building an application like the one discussed in Chapter 7, it is not only the security features of the Smart Card that will make it a success. The advanced security of the Smart Card is the driver for using this technology. There are a few other aspects that should be considered: human readable security features, security features of the Smart Card chip, security features of the operating system, security features of the network and security features of the application (see [8]).

Besides the advantage of strong security that Smart Cards offer, they also have more storage space and a processor. This is the next point to be discussed.

2.2.3 Advanced Processing and Storage Capabilities of Smart Cards

The processing capabilities of a Smart Card makes it immune to eavesdropping, because the user's secret key and the system's secret key will not be used outside of the card, they stay inside the card where they are protected and secure (see [4]).

Most Smart Cards these days have a storage capacity of about 8-32 kilo bytes. This storage capacity is divided into 2 files that are used: the internal and user files (see [2]).

2.2.3.1 The Internal Files

These files contain all the information about the configuration of the card. This information will never be seen by the user. The internal files can be accessed by presenting the IC (Issuer Code). When the IC is presented, security configuration on the card can be changed. These configurations include the use of DES or triple DES (discussed in Appendix A and B).

Data can be encrypted or viewed as plain text. Encryption is the safer and preferred option. Security settings that can be encrypted include the IC, PIN, and AC1 – AC5 (discussed below, see [2]). All of these are configuration settings on the card.

2.2.3.1.1 IC

This is the Issuer Code that is needed to go into another stage of the card (discussed in section 2.2.5). This code is 8 bytes long.

2.2.3.1.2 PIN

The pin is used to control access to the data on the card and is 8 bytes long.

2.2.3.1.3 AC

This stands for application codes. These five codes, AC1 – AC5, are used to control access to the data stored in the data files on the card. Each one is 8 bytes long.

A Smart Card's storage is divided into two files types, internal and user files. We have now looked at the internal files. Next we will take a look at the user files (see [2]).

2.2.3.2 The User Files

These files are where all the users' information will be stored. This is the data that the card reader will read and this is where the fingerprint template will be stored.

We have now discussed files and processing capabilities of a Smart Card. But these two aspects need to be managed. This is where the Chip Operating System comes in (see [2]).

2.2.4 Chip Operating System

Smart Cards have a micro processor, memory and files. All of these components need to be managed, and for that the COS (Chip Operating System) is used. The COS handles the files; manages the memory and the data transmission protocol. More importantly, the COS also makes sure that the data on the card can only be accessed through certain gates, thus making sure that the data remains tamper free (see [4]). By ensuring that the data is only accessed in the right way, only the right person with the correct keys and codes (IC code) can change the data on the card, ensuring better security and privacy (see [2]).

The last aspect of Smart Cards that we will look at is the life stages that a Smart Card can exist in.

2.2.5 Three Life Stages of a Smart Card

A Smart Card can exist in three stages (see [2]), the Manufacturing stage, Personalization stage and the User stage. In each stage the use of the Smart Card differs. We will start by looking at the first stage, the Manufacturing stage.

2.2.5.1 The Manufacturing Stage

This is the first stage that a card can exist in, and when this stage is finalized, the stage can't be entered again. The Issuer Code(IC) is written to the card. The IC is later used to enter the personalization stage. This stage is over as soon as the manufacturer fuse has been programmed. The manufacturing fuse is a bit that is programmed to the EEPROM. This bit is irreversible (see [2]).

The second stage that a Smart Card will exist in is the Personalization stage (see [2]).

2.2.5.2 The Personalization Stage

In this stage the card is configured and all the security settings are assigned. This stage is over when the personalization bit is programmed to the EEPROM. To re-enter this stage the IC is needed. The data on the card can be cleared and the card can be formatted.

The last stage of a Smart Card is the User stage. This is the final stage of a Smart Cards life. For the Smart Card to be used, it must be in this stage (see [2]).

2.2.5.3 The User Stage

This is the stage when the card is in operation and data can only be read. To change the data, the IC (Issuer Code) that was programmed to the card in the Manufacturing stage needs to be presented to enter a special Issuer Mode. In this mode we have access to all the data files. We can now write data to the files (see [2]).

We have now looked at different Smart Card types that are available and discussed a few aspects of Smart Cards. In the next section we will take a look at the advantages and disadvantages of Smart Cards.

2.3 Advantages and Disadvantages of Smart Cards

Smart Cards have certain advantages over other card types that make them better choices for a lot of applications. Smart Cards can do more than other cards, and they can do it better. We will start by first looking at the advantages that Smart Cards have.

2.3.1 Advantages of Smart Cards

The first advantage of Smart Cards that we will look at is the increased memory space that they have.

2.3.1.1 Memory Space

Smart Cards have more memory space than any other card technology available today. They can store between 8 and 32 kilo bytes (see [5]), depending on the card type, that is about 800 times more than the magnetic stripe card.

The second advantage of Smart Cards that we will look at is the processing capabilities.

2.3.1.2 Processor Capabilities

The Smart Card is able to do operations on data, can alter the data and store them. Smart Cards can authenticate people offline by inserting the Smart Card and then providing a pin or biometric that is stored on the card (see [1]).

The processor of the Smart Card provides it with better security. That's the next advantage of using Smart Cards.

2.3.1.3 Advanced Security and Data Privacy

Data is stored on the card and is encrypted using DES or triple DES and MAC is used to check the integrity (discussed in Appendix A, B and C respectively). Another security feature is that Smart Cards can be combined with biometrics. The biometric template can then be stored on the Smart Card (see [4]).

The security of Smart Cards will help to decrease fraud when used in financial applications (see [9]).

With the advanced security of Smart Cards, they can be used for multi application cards without data being mixed.

2.3.1.4 Multi Application Cards

One card can be used for more than one application. For example, one card can be used for access control and an electronic wallet (see [7]). This would help to reduce the number of cards that people need to carry with them. The data of the two applications are separated by a firewall to stop any unauthorised access to the data (see [8]).

The fifth advantage of Smart Cards is that they reduce cash in hand for users when used as a financial card.

2.3.1.5 Reduce Cash in Hand

Reduced cash in hand for people makes it safer against theft (see [3]). Transaction costs of cash in hand are more than the cost of electronic transactions.

The last advantage that we will discuss is the mobility of the Smart Card.

2.3.1.6 Mobility of Smart Cards

The card can be used at various places and still offer the advanced security. The data is on the card and not confined to a central database where a connection would be needed to retrieve the data (see [8]).

We have now discussed six advantages of Smart Cards. In the next section we will take a look at some of the disadvantages of these cards.

2.3.2 Disadvantages of Smart Cards

The first disadvantage of Smart Cards that we will look at will be the wear and tear of contact Smart Cards.

2.3.2.1 Wear and Tear

Contact Smart Cards have a lot of wear and tear due to the fact that they need to be inserted into a reader (see [10]). The gold plated chip takes a lot of scratching and this can damage the card and will reduce the card's lifetime. The contact less Smart Card does not have the same problem.

The next problem of Smart Cards that we will discuss is electrostatic discharges.

2.3.2.2 Electrostatic Discharges

This may damage the card permanently (see [10]). This is caused when electric currents flow from the reader to the card and the two devices are on different electric potentials. The different electric potential in the card could be caused by static electricity.

The next disadvantage of Smart Cards that might cause people to be hesitant to use this technology is the fear that a transaction will be done without their knowledge.

2.3.2.3 Transactions without User Authority

With Contact Less Smart Cards people can be scared that they do a transaction without their knowledge (see [10]). Usually contact less Smart Cards won't be used for such applications.

The last disadvantage that we will look at is the lifestyle of a person.

2.3.2.4 Lifestyle

A disadvantage specific to this dissertation will be student life. While a card is in a student's pocket, there is a chance that the card can get wet, or the card can be bending in unusual ways. All of this can damage the card or the microprocessor.

Smart Cards have a few disadvantages, but the advantages definitely outweigh the disadvantages, making Smart Cards a good choice depending on the application and the environment where they are to be used.

In our next section we will discuss the components that make up a Smart Card.

2.4 Components of a Smart Card

Smart Cards consist of several parts that are integrated and working together as one. All of these components come in one plastic card that is the size shown in the diagram below. The smaller square on the inside is the gold plated chip, or also known as the interface. This chip is where most of the components are and where all the operations happen.

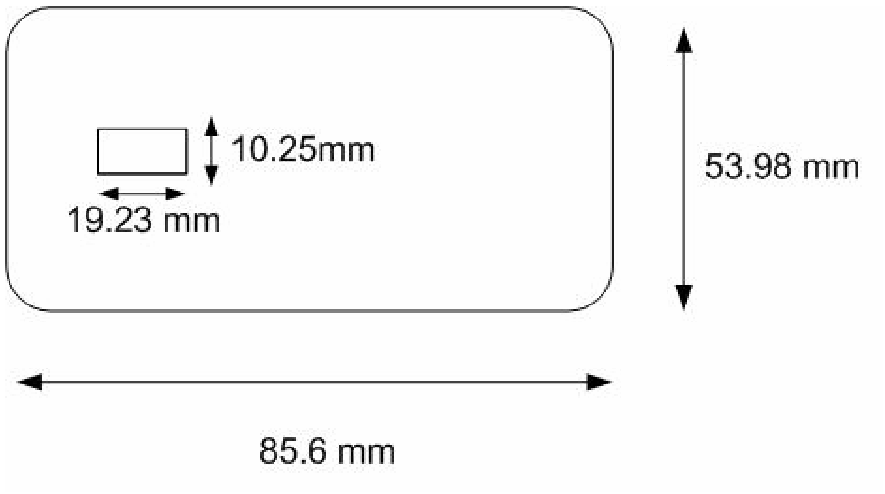


Figure 2.2: Dimensions of a Smart Card and the integrated circuits chip

Smart Cards consist of **7 components**, and we'll start by looking at the outer body (for section 2.4.1 to 2.4.7 see [5]).

2.4.1 Carrier (Body)

This is the plastic card that you see when holding the Smart Card. It is usually made of plastic and must protect the chip. The plastic body is one of the restrictions on Smart Card improvement, because a better processor and more memory would increase the heat and that can cause the plastic to melt.

The rest of the components are on the gold plated chip that can be found on a Smart Card. The first component on the gold chip that we will look at is the ROM.

2.4.2 ROM

The Read Only Memory has a size of about 2-16kb (depending on the card). The ROM stores the COS that manages memory usage, files, data and the transmission protocol. The programmer is not able to erase this memory, as he won't be able to replace the COS.

The third component of a Smart Card is the EEPROM.

2.4.3 EEPROM

The Electrically Erasable Read Only Memory is similar to a computer's hard drive. Its size may vary between 2-32kb depending on the card. This is where the user's information will be stored on the card. This memory can be erased by the programmer, and new data can be stored on the EEPROM.

The next component that we will discuss is PROM.

2.4.4 PROM

Programmable Read Only Memory loads the serial numbers of the card. The size of this memory is 32 bytes.

As with any computer with a processor, RAM is needed for faster access of data. The next component is RAM.

2.4.5 RAM

The Random Access Memory, also known as volatile memory, will do pretty much the same as RAM in a pc. Some data and instructions will be loaded into the RAM, because the RAM is closer to the processor than the ROM and RAM is a lot faster. The size can be anything between 128-512 bytes.

The next component is one of the most important components on a Smart Card, the processor. The processor provides the Smart Card with most of its advantages over any other card technology.

2.4.6 Processor

This is an 8 bit processor that has a clock speed of about 5 MHz. The architecture is CISC (Complex Instruction Set Computer). The CISC architecture allows for the execution of several low level instructions in one CISC instruction. The low level instructions include arithmetic instructions, load and save in memory.

The last component of a Smart Card is the interface.

2.4.7 I/O Interface

The input/output interface has a data flow rate of 9600bits/sec. The gold plated ship is divided into 7 sectors, and one of these sectors is the I/O Interface. It is thus only this small part of the chip where data flows through.

With all of these components working together, some standard is needed. In the next section we will discuss some standards that are applicable to Smart Cards.

2.5 Smart Card Standards

Most of the standards that exist for Smart Cards and the Smart Card readers are managed by ISO, the International Standards Organisation (see [32]). They define sizes, strength, power use and location of certain components for the devices, just to name a few.

We will start by looking at the ISO 7816 standard.

2.5.1 ISO 7816

This standard is divided into three parts, each handling a different section of standards for Smart Cards (see [7]). To conform to ISO

7816, the Smart Card must conform to all three parts (see [7]). We start by looking at part 1 of ISO 7816.

2.5.1.1 ISO 7816 Part 1

This is a follow on of ISO 7810. Part 1 defines the **physical characteristics** of Smart Cards. This includes the mechanical strength of the card, surrounding temperature, physical dimensions and the resistance of the contacts.

Part 1 also describes how the card would function and react to **exposure of certain forces**. These forces are X-Rays, UV light, static electricity and electromagnetic fields.

This card can, and in some cases will be subject to a **lot of strain** being put on the card. The card can go through a washing machine, can be sat on while in the back pocket of a pair of pants and can even be left in extreme temperatures. All of this has to do with the mechanical strength of the card.

The next part of the ISO 7816 standard for Smart Cards that we will discuss is part 2.

2.5.1.2 ISO 7816 Part 2

This standard is a follow on of ISO 7811. This part defines the arrangement of the chip, location of the embossing, location of the contacts and the dimensions of the contacts.

Part 2 also defines the function of the 8 parts that are on a chip (called C1 – C8).
C1: **VCC**: power connection for the microprocessor.
C2: **RST**: reset line.
C3: **CLK**: clock signal line for microprocessor’s clock speed.
C4: **RFU**: reserved for future use.
C5: **GND**: ground line.

C6: **VPP**: power connection for EEPROM.

C7: **I/O**: input/output line.

C8: **RFU**: reserved for future use.

The last part of the ISO 7816 standard that we will look at is part 3.

2.5.1.3 ISO 7816 Part 3

Part 3 defines the communication protocol, structure of answer to reset (ATR), basic electrical characteristics and functions of various contacts on the Smart Card. This is one of the most important specifications.

Part 3 deals with a few factors:

1. electrical signals,
2. voltage and the current value that the part of the chip (C1 – C8) could be in,
3. the operating procedures for Smart Cards,
    a. Connection and activation of Smart Card,
    b. Reset the card,
    c. ATR by the card,
    d. Exchange of information,
    e. Deactivation of the contacts,
4. answer to reset (ATR),
5. protocol type selection,
6. protocol type T=0.

Now that we have briefly discussed the ISO 7816 standard, we will move on to the next leading standard that regulates Smart Cards. The GSM standard focuses on Smart Cards used in cell phones, better known as SIM cards.

2.5.2 GSM

Originally from Groupe Special Mobile, GSM stands for Global System for Mobile Communications. GSM is divided into two parts dealing with the functional characteristics of the GSM network and also the characteristics of the SIM card (see [4]). The newest trend is to use a Smart Card as the SIM card (see [8]).

The third standard that regulates Smart Cards and their components that we will discuss is EMV.

2.5.3 EMV

EMV stands for Europay International, MasterCard International and Visa International (see [4]). This is another document for Smart Card standards. EMV is divided into three subsections covering Smart Card design aspects, Smart Card terminal design aspects and debit/credit applications on Smart Cards (see [8]).

This standard allows for interoperability across different vendors. EMV can be seen as an extension to ISO 7816, but EMV is only applicable to financial applications. We will discuss in short the three subsections of the EMV standard (see [10]). Smart Card design aspects are covered in section 1.

2.5.3.1 Section 1: Smart Card Design Aspects

This covers electromechanical properties, card session, the answer to reset and transmission protocols (see [10]).

The second section of the EMV standard covers terminal design aspects.

2.5.3.2 Section 2: Smart Card Terminal Design Aspects

This section covers security, card holder and acquirer interface, general physical characteristics of the card terminal and software and data management (see [10]), which will be handled by the Chip Operating System (COS).

The last section of EMV is for financial applications.

2.5.3.3 Section 3: Debit/Credit Applications on Smart Cards

This section covers the transaction flow and exception handling (see [10]).

It is clear that a lot of the specifications in EMV are also in ISO 7816, but as mentioned, EMV is an extension of the ISO 7816 standard, and is specifically designed for financial applications.

Our fourth standard for Smart Cards and the readers is the PC/SC standard.

2.5.4 PC/SC

PC/SC stands for Personal Computer/ Smart Card (see [4]). This is a set of standards for the integration of Smart Cards to computers.

This standard is divided into 10 parts and can be downloaded for free from http://www.pcscworkgroup.com/

This is a quick list of all the parts of this standard:

1. Introduction and Architecture Overview
2. Interface Requirements for Compatible IC Cards and Readers
3. Requirements for PC-Connected Interface Devices
4. IFD Design Considerations and Reference Design Information
5. ICC Resource Manager Definition
6. ICC Services Provider Interface Definition
7. Application Domain/Developer Design Considerations
8. Recommendations for ICC Security and Privacy Devices
9. IFD with Extended Capabilities
10. IFD with Secure Pin Entry Capabilities

The last Smart Card standard that deserves a mention is the ISO 7813 for financial applications.

2.5.5 ISO 7813: Financial Transaction

A Smart Card can be used as a financial card, for example a credit card. This standard will then regulate the security features that must be enforced on the card to protect the data.

2.6 Summary

In this chapter we have discussed the four different types of Smart Cards that exist namely: contact, contact less, hybrid and combination cards.

Smart Cards have better and stronger security than any other card technology that exists today. With a processor on the card and storage space of between 8 and 32 kb, Smart Cards are a big improvement in the card technology industry.

Data on Smart Cards can only be accessed through certain gates. This is controlled by the Chip Operating System (COS). The COS manages the data access, the internal and user files and the memory of the Smart Card.

A Smart Card can exist in three life stages: the manufacturer stage, the personalization stage and the user stage. When in the user mode the Issuer Code can be submitted to enter an Issuer Mode. In the Issuer Mode the data in the user files can be changed.

We identified several advantages and disadvantages of Smart Cards, and saw that the advantages outweigh the disadvantages. The advantages of Smart Cards will improve the security and capabilities of applications that make use of Smart Cards. Smart Cards can be used as multi application cards.

A Smart Card consists of a lot of small components functioning together. The 7 components that form a Smart Card are: the carrier (body), ROM, RAM, EEPROM, PROM, Processor and the I/O Interface.

In the last section we had a look at five standards that regulate Smart Cards. Standards regulate the sizes of some of the components, their placement on the Smart Card and the operating procedures of Smart Cards. The first standard ISO 7816 has three parts that deal with Smart Cards.

The GSM standard was developed specifically for use of Smart Cards (SIM card) in cell phones.

Other standards include EMV, PC/SC and the ISO 7813 financial standard.

Now that we know more about Smart Cards, we need to take a look at other card technologies that can and are being used as student cards.

Chapter 3: Typical Student Card Types

3.1 Introduction

Various types of card technologies have been used as student cards, and some are still being used today. Although these cards are inferior to Smart Cards, they still served their purpose as a student card.

In this chapter we will take a look at the magnetic stripe card and the RFID card, as both have been used in the University environment. We will discuss the card technology, how the card works, take a look at the system and try to identify any advantages and disadvantages of that system.

3.2 Magnetic Stripe Cards

Magnetic stripe cards look like any other card that is used today, with one small exception, the black stripe on the back of the card (as shown in the picture below).

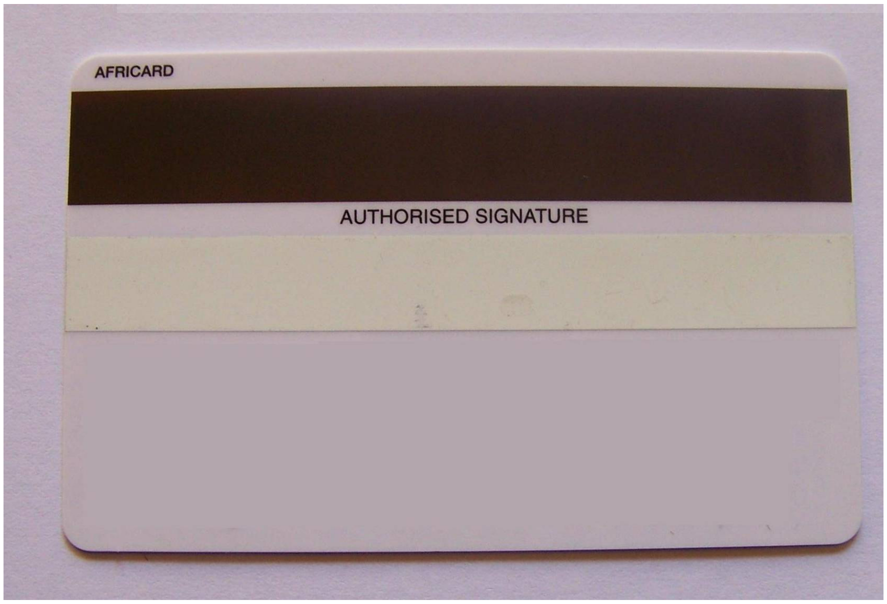


Figure 3.1: A plastic magnetic stripe card

3.2.1 The Black Magnetic Stripe

This stripe consists of two to three tracks of magnetic particles (see [8]). The track is then divided into several domains. These domains will hold the data in machine readable format. This is achieved by magnetizing a domain, giving it the value of 1, or leaving it untouched, giving it the value 0 (see [10]). This will yield data in binary format.

A protective layer will be placed on the outside of the tracks.

Two types of materials are used for the tracks on a magnetic stripe card (see [8]):

3.2.1.1 Low-coercivity (LoCo).

This material can be magnetized by a relatively weak magnetic field. This is the older of the two materials.

LoCo is subject to counterfeiting. The technology used to magnetize LoCo is very cheap and can be purchased by anyone (see [8]).

The second material that can be used for the track is High-coercivity.

3.2.1.2 High-coercivity (HiCo).

This is the newer technology and is preferred by all the big companies for their cards.

HiCo requires a stronger magnetic field for magnetizing the tracks on the card. The technology used is expensive and potential buyers of the technology would need to state their reasons for purchasing the technology (see [8]).

The advantages of HiCo over LoCo don't stop at the minimization of counterfeiting of the cards. HiCo also has better resistance to external magnetic fields and the exposure to heat.

The process used to encode magnetic stripe cards is called F/2F (see [8]). All the cards are encoded using this process, allowing any magnetic card reader to read any of the cards.

We will now take a look at the advantages and disadvantages of magnetic stripe card technology. We start by discussing the disadvantages.

3.2.2 Disadvantages of the Magnetic Stripe Card

The first disadvantage that we will look at is the fact that the card needs to be swiped.

3.2.2.1 The Card Needs to be Swiped

All magnetic stripe cards must be swiped through a reader for authentication. In the case of credit cards the user inserts the card into the reader before proceeding. This is time consuming for applications that need a high throughput.

The next problem with magnetic cards is the small storage space they offer for data storage.

3.2.2.2 Small Storage Space

The available storage for data is in the range of 900 – 1000 bytes (see [10]). This is considerably smaller than the Smart Card and this puts a constraint on the applications that the card can be used for.

The third disadvantage of magnetic cards is only a disadvantage when compared to Smart Cards. They can’t be used as a multi application card.

3.2.2.3 The Card can’t be used as a Multi Application Card

The fact that the card doesn’t have a processor and the limitations on storage means that the card can only be used for one application.

The last disadvantage is also when magnetic stripe cards are compared to Smart Cards. Their lack of security features.

3.2.2.4 The Lack of Security Features

The cards are counterfeited by copying the data bit for bit (known as Skimming, see [10]). There is no way for the card to enforce its own security measures.

Human readable security features is the only way to try and minimize the damage. This includes a photo of the owner on the card and small text printed on the card that can’t be reprinted.

The disadvantages place several constraints on the applications and the use of the card. More effort is required from the computer’s side. The computer should provide the security and more storage.

We will now discuss some of the advantages of magnetic stripe cards.

3.2.3 Advantages of the Magnetic Stripe Card

The first advantage of this technology is the price for cards and readers.

3.2.3.1 These Cards are Inexpensive

This allows them to be used as disposable cards. A lot of money is saved when buying these cards because they are so cheap (see [35]).

The other advantage of magnetic stripe card technology is their reliability.

3.2.3.2 They are Reliable

There is no tag or microprocessor in them that can fail or that needs power.

Magnetic stripe cards are regulated by the ISO 7811 standard.

Magnetic stripe cards isn't the only card technology that are used as student cards. RFID is a popular technology for the purpose of access control. We will now discuss RFID cards.

3.3 RFID Cards

Radio Frequency Identification (RFID) cards look like a normal plastic card, with no visible connection interface on the card (as shown in the picture below).

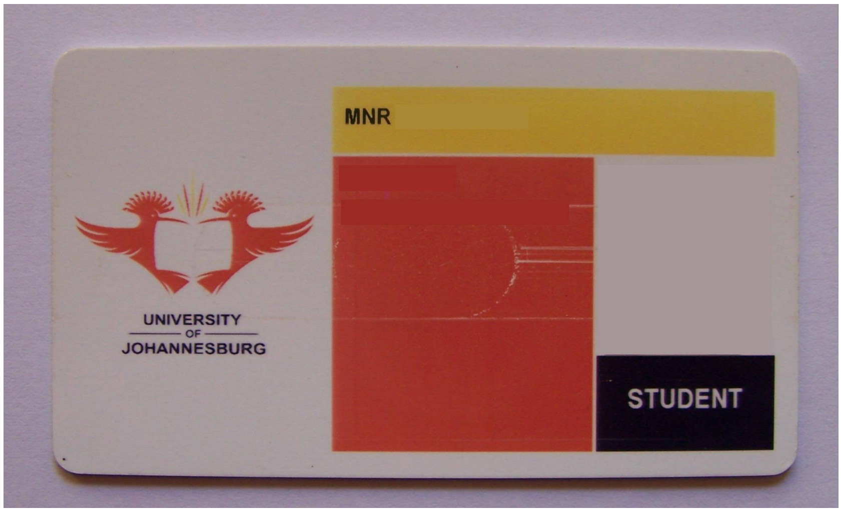


Figure 3.2: The RFID card that the University of Johannesburg uses

We will now take a look at RFID as a contact less technology and the components that it consists of.

3.3.1 RFID is a Contact Less Technology

Inside the card there is a small micro chip or tag, this is protected by the plastic cover. This technology allows that the card only needs to be in the region of the reader to be picked up. The distance between the RFID card and the reader depends on six factors (see [11]).

We will take a quick look at these six factors that determine the distance in which a card and a reader can see each other. We start by looking at the power of the transmitter on the reader.

3.3.1.1 Power of the Transmitter of the Reader

A more powerful transmitter would allow for longer ranges that the card will be picked up in. Most passive systems (discussed in chapter 3.3.3) have a range on a few centimetres to 3 or 4 meters. A more powerful transmitter would allow the card to return a stronger signal to the reader (see [11]).

The next factor that determines the distance between a card and a reader is also found on the reader, the receiver.

3.3.1.2 The Sensitivity of the Receiver of the Reader

This determines how well the reader can pick up signals. Weaker signals would require a more sensitive receiver (see [11]).

The third and last factor that depends on the reader is the antenna gain.

3.3.1.3 The Antenna Gain of the Reader

A bigger, larger antenna would increase the range. For passive systems this can take up space (see [11]).

The next three factors that determine the distance between the reader and the card all depends on the card. We start by looking the antenna gain of the card.

3.3.1.4 The Antenna Gain of the Card

This is basically the same as for the reader. In the card there is not place for a bigger antenna. This would also require more power, and power is limited by the signal (see [11]).

Now we will take a look at the power requirements of the card and the influence that this has on the distance between the card and the reader.

3.3.1.5 The Power Requirement of the Card

Passive cards get their power from the Radio Frequency (RF) signal, and then use this power to send a reply to the reader. Longer distances would require more power for the reply signal (see [11]).

The last factor is the efficiency of the card modulator. A more efficient modulator will be able to handle longer distances between the card and the reader.

3.3.1.6 The Efficiency of the Card Modulator

This depends on the signal that is send back to the reader, and what method is used to send the signal. The efficiency is also dependent on the power available (see [11]).

The signal of the reader and the card can be read through various types of materials, no direct line of sight is needed (see [13]), but the signal can be affected by certain factors in the environment. Any material between the reader and the card will affect the strength of the signal. There are however, certain materials that won’t let any signals through or just rebound the signal away from the card or reader (see [11]). They are water (a really wet material may yield the same result) and metal (a layer of tin foil).

These two materials generally don’t come into play in the University environment, and even if they do, shouldn’t pose any problems. The card can simply be removed from the problem area (a wallet) and presented with no interference of the signal.

3.3.2 Types of RFID Technologies

Three types of RFID technologies exist today: the active, passive and semi-passive RFID tags (see [12]).

We will now discuss these three RFID technologies by starting with a look at the active tag.

3.3.2.1 Active Tag

This means that the tag or card has an onboard battery providing the power (see [13]). The only problem being that the battery has to be changed when flat.

The signal strength is stronger in active RFID, which means that the range of communication is bigger, even a few hundred meters. The tag can move at 160kph and the data will be read successfully. Active RFID has the largest storage capacity of all the types, with128k bytes of available storage.

This is the most reliable RFID – it doesn't need a radio signal to be powered (see [11]).

The second type of RFID tag that we will discuss is the passive tag.

3.3.2.2 Passive Tag

The tag or card has no power of its own. It needs power from the reader, where power is extracted from the signal (see [13]). Higher powered readers are needed for passive cards.

These tags are slower because of the low level of power. The low power shortens the communication distance from a few centimetres to about 3 meters.

Passive tags have about 128 bytes of storage available. This tag is smaller and cheaper than the others, and has a longer life (see [11]).

Now that we have discussed Active and Passive RFID tags, we will discuss the third type of RFID tag. This is a combination of the other two, and is known as the semi-passive tag.

3.3.2.3 Semi-passive Tag

This is a combination of the two tags discussed above. It has a battery that it only uses to send out a stronger signal when replying to a reader. This RFID isn't always sending out a signal, it only responds to a reader (see [12]).

3.3.3 RFID Components

RFID technology consists of 3 components: RFID tag (transponder), the reader (transceiver) and the antennas and radios (see [13]).

We will start this discussion by looking at the first component, the tag.

3.3.3.1 Tags

This is the part that responds to a reader's signal. Some tags can respond to any reader, others are more secure. The secure tags need some form of authentication from the reader before it can respond (see [11]).

A tag consists of the following two parts (see [13]):

1. Antenna,
2. A small silicone chip.

The silicone chip consists of (see [11]):

1. Radio receiver,
2. Radio modulator,
3. Control logic,
4. Some memory,
5. Power system (active or passive).

Three types of tag memory exist (see [12]):

1. Read Only (RO) are pre-programmed tags,
2. Write One Read Many (WORM) are pre-programmed, but data can be added later,

3. Read Write (RW) where data can be added at any given time.

Data that is stored on the card’s memory include the unique serial number of the card. Other data can be stored in the memory as needed for the application. The stored data is called the ID of the tag, and in most cases it is 96 bits in length (see [13]).

When a reader has more than one tag in its range that it needs to read, it either uses an anti-collision or singulation protocol.

3.3.3.1.1 Anti-collision Protocol

Each tag responds at a random time to the reader, this gives the reader time to register and read them all. When a collision still occurs, the parties involved in the collision are notified of the problem. They respond again at another random time interval (see [13]).

3.3.3.1.2 Singulation Protocol

The reader has a list of all the tags in his range that needs to be read. The reader works through the list like a binary tree, and thus reading all the tags one by one (see [11]).

We will now take a look at the second component of RFID technology, the reader.

3.3.3.2 Readers

RFID readers constantly send out an RF signal, looking for tags to respond. The region of this RF signal is also known as the interrogation zone (see [12]). The RF signal from the reader can contain passwords for authentication, certain commands and even read and write instructions (see [11]).

The readers come in many sizes depending on the application they will be used for.

The last component of RFID that we will discuss is the antenna and radio.

3.3.3.3 Antennas and Radios

These are the main components for the communication between the tag and the reader. Larger antennas will make the whole system function better and more efficiently. A larger antenna on the reader will allow more power to be sent to the tag in a passive tag environment. A larger antenna on the tag will improve the signal that is sent back to the reader (see [11]).

Radio energy from an antenna can be measured in two ways (see [11]):

1. The frequency at which the signal oscillates,
2. The strength of the power of those oscillations.

The RF wave length that will be used depends on the application that the RFID will be used for (see [11]).

Low-Frequency (LF) and High-Frequency (HF): Animal tagging and keyless entry.

Ultrahigh-Frequency (UHF): Smart Cards, logistics and item management.

Industrial, Scientific and Medical band (ISM): item management.

RFID uses the unlicensed radio frequency spectrum.

In the next section we will take a look at advantages and disadvantages of the RFID technology. We will start by discussing some of the disadvantages.

3.3.4 Disadvantages of RFID Technology

The first disadvantage of RFID is that the tags aren't protected. There is no security for the tag or the data.

3.3.4.1 Unprotected RFID Tags

Unprotected tags are vulnerable to counterfeiting, eavesdropping, physical attacks, spoofing and denial of service attacks (DOS, see [13]).

The second disadvantage is the battery life of these tags.

3.3.4.2 Battery Life

An active RFID has a battery that can pose a problem. The battery can run flat at an unexpected time (see [11]).

The last disadvantage of RFID tags that we will look at is when signals are blocked.

3.3.4.3 Materials Blocking the Signal

Certain materials like metal and water can be used to block the signal from the reader. This can be used as an attack on the technology (see [13]).

We will now discuss some of the advantages that RFID technology has.

3.3.5 Advantages of RFID Technology

A big advantage of RFID is that no contact is needed.

3.3.5.1 Contact Less Technology

This technology has a high throughput and no wear and tear (see [13]).

Since RFID is a relatively old technology it has the advantage of being cheap.

3.3.5.2 Cheap with a Long Life Time

The passive tag has a long lifetime and is quite cheap to produce (see [11]).

As mentioned earlier, RFID has a high throughput rate. This is because no line of sight is needed between the reader and the tag. This brings us to the next advantage of RFID.

3.3.5.3 No Line of Sight Needed

Because the reader and the card emit a RF signal, the signal can be read through certain materials (see [13]). The tag can be placed in a wallet and still respond to the reader.

The last advantage of this technology that we will discuss is the reading of multiple tags by one reader.

3.3.5.4 Reading of multiple tags

One reader can read multiple tags in a short time. This is done by using an anti-collision or singulation protocol (see [11]).

RFID is regulated by the ISO 15693 standard (see [12]).

3.4 Summary

This chapter looked at other card technologies that can be used as a University student card. The first technology that we discussed was the Magnetic Stripe Card.

Two types of materials can be used for the black magnetic stripe on the back of the card: Low-coercivity and High-coercivity. It is easier to counterfeit Low-coercivity cards.

Magnetic stripe cards have the advantage of being reliable and inexpensive. But they also have a few disadvantages, like no security features and small storage space.

The second type of card technology that we discussed was RFID (Radio Frequency Identification Cards). The types of RFID tags that are available for use today are: Active, Passive and Semi-passive tags.

There are a few factors that play a role in determining the distance that a tag and reader can communicate with each other. These factors on the tag reader's side are: power of transmitter, sensitivity of the receiver and the antenna gain. Factors on the tag's side are: antenna gain, power requirement and efficiency of the modulator.

RFID consist of 3 components, this includes the tag, the reader and the antenna and radio.

The last section took a look at some of the advantages and disadvantages of RFID technology. Access control is not necessarily the best application for RFID, but it does work really well.

We now know a little more about other card technology systems that were used as University student cards.

This whole dissertation is about Smart Cards and the Smart Card VeriSys system. With that in mind, we will now turn our focus back to Smart Cards.

In the next chapter we will find other applications that Smart Cards are used for. Each application will be discussed in short.

Chapter 4: Other Smart Card Applications and their Functionality

4.1 Introduction

With the functionality and advantages that Smart Cards offer over other card types, they are being used for a wide variety of applications. Different countries have different uses for Smart Cards. Europe is leading in the use of Smart Cards with America a long way behind.

In most of the applications the Smart Card is used to **store sensitive data** on the card, the type of data that a person doesn't want to be compromised (see [14]). In some cases the card is used as a multi application card. This helps reduce the number of cards that are issued, and people have less cards to worry about.

The rest of the chapter will concentrate on other applications that Smart Cards are used for, and we will discuss these applications in short.

The first application that we will look at is the payphone card.

4.2 Payphone Card

The use of a Smart Card for payphone purposes are one of the most common uses for Smart Cards (see [36]).

The payphone of a few years back used **money and coins to operate**. The problem was that the user always needed change to make a call, and sometimes certain coins won't be accepted by the machine. But this was not the biggest issue. A bigger problem existed: the fact that the exact change was needed when you ended a call. This wasn't always possible.

Smart Cards offered another solution. A card can be bought with a fixed amount of money loaded onto the card. This card is then used to pay for the call. This solved the problem of change and a machine won't reject the card as is the case with coins.

Smart Card as a payphone card can be used in one of two ways:

1. **Disposable card**. When all the money is used, the card can be thrown away.
2. **Reusable card**. This card can be used again and again. The user can load money onto the card at any time, and as mush credit as needed.

The second application of Smart Cards that we will look at is the SIM card.

4.3 SIM Card

The SIM card that is found in cell phones is the other common use for Smart Cards. Although there are small differences between a normal Smart Card and the SIM, they are changing and becoming more and more identical to each other (see [4]).

The SIM is used to store the phonebook, messages and applications that are used by the phone. Memory cards are available that can store the data. The cell phone just acts as an interface between the user and the Smart Card.

This area of application uses the biggest amount of Smart Cards of all the applications. **SIM cards use the power of Smart Cards** to the best effect, with applications running on a phone (see [4]) and the need for the card to support GSM instructions.

Another area of applications where Smart Cards are big is the financial sector.

4.4 Financial Cards

Smart Cards can be used as credit cards, debit cards or a digital money card (see [4]). This allows us to view information of the account a lot easier and less paper work is involved (see [7]).

The use of Smart Cards will help to improve customer service. Smart Cards will provide a **faster and more secure** way of internet banking (see [7]).

We will now discuss three financial cards that a Smart Card can be used for, starting with credit cards (see [9]).

4.4.1 Credit Cards

With credit cards the user swipes the card, the transaction goes through, but the user then owes the bank the money. The payment is made later to the bank as the user places money onto the card (see [9]).

The second financial card that we will look at is the debit card.

4.4.2 Debit cards

These cards must have money on them for the user to make a payment or to do a transaction. This is a pay now type of system, where money on the card is needed (see [9]).

The last financial card that we will discuss is the digital money card.

4.4.3 Digital money card

With the digital money card the user spends the digital money that is available on the card. This digital money can be earned in the form of loyalty points and then spent on a variety of items (see [9]).

A big problem with digital money is that it can **easily be copied**. The process is a lot easier than with real money. Copying the digital money is as simple as copying a series of bits (see [4]).

In the next section we will discuss some of the advantages that Smart Cards will give us when they are used as financial cards.

4.4.4 Advantage of a Smart Card as a Financial Card

The first advantage is that the software on the Smart Card can't be illegally accessed and altered.

4.4.4.1 Smart Card is Tamper Resistant

The software will remain authentic, meaning that we can be sure that when money is removed from the card that it is actually removed (see [4]). When money is moved from one card to another, we can be sure that the money is removed from the first card and that a copy isn't kept on the card.

For financial applications a Smart Card can be combined with a biometric property to be even more secure.

4.4.4.2 Smart Card Combined with Biometrics

Smart Cards combined with biometrics and/or a pin will provide even better security to the user. Essentially Smart Cards provide offline authentication that makes it more secure against fraud and tampering. This helps to secure a customer's accounts and transactions (see [9]).

The third advantage of a Smart Card as a financial card is the processing capabilities of the Smart Card.

4.4.4.3 Processor

The processor on the card also helps with security, and the hardware can't be removed from card to be changed or tampered with (see [4]). There is only one way to get to the data on the card and that is through the COS (Chip Operating System).

Smart Cards have huge potential as a financial card and will improve the security for the bank and their clients.

The next Smart Card application that we will look at is the medical card.

4.5 Medical Card

A big problem in the medical sector is the **privacy of a patient's medical records**. It is against the law to make a medical record or any details thereof public. Thus the security of these records can become a headache for anyone working with it.

Smart Cards that store the patient's medical record on the card will help to keep it safe and secure. In the case of an emergency the data will be available quicker for faster treatment to the patient (see [7]).

The use of Smart Cards will cause **databases to be smaller**, cheaper and easier to maintain (see [7]). They also offer a convenient way to move data between different systems, no need for the systems to be connected (see [7]).

We will now discuss the Smart Card as a social card, the fifth Smart Card application in this chapter.

4.6 Social (ID) Card

The social or ID card is a card that can contain information like ID number, drivers' license, passport and even firearm licenses (see [36]). This card will replace the ID document and a few others that still exist in a lot of countries today. A new trend in Europe is to use the Smart Card as an electronic passport.

The advantage of a card like this is that it is an **all in one card**. Only one card is needed for every thing.

With the use of Smart Cards, the person’s information will be kept secret in the same way as with medical cards. The card can once again be combined with passwords or biometrics to make stolen cards useless.

The next Smart Card application that we will discuss is the loyalty card.

4.7 Loyalty Card

Loyalty cards are a **point based system** where companies reward customers with points when they make purchases at their store (see [7]). The bigger the value of the purchase, the bigger amount of reward points will be earned. These points can then be exchanged for gifts or for discount on the next purchase. This will hopefully encourage the customers to purchase more at their store since they get a reward.

A lot of companies have joined forces and are giving out one loyalty card to all of their customers. The customers can then use this card to earn points at any of the participating stores. Competing companies won’t join forces, but a chain shopping store and a hotel might.

Points can be earned in any retail way, for instance at point of sale systems or when booking in at a hotel. Other uses can include the entertainment industry, parking lots and the paying of services offered to the customer (see [7]).

Smart Cards can help people to **spend the points** on many more different ways. Smart Cards will also allow more companies to join in the shared loyalty card because of the increased memory space it offers (see [4]).

The next section will concentrate on access control applications using Smart Cards. These applications will definitely benefit from Smart Cards. Access control will be more secure.

4.8 Access Control

Access control is the controlling of access to property, use of hardware or machinery and the **protection of information and data** (see [7]). For a person to get access to these protected resources he needs security clearance.

In the past, proximity cards and magnetic stripe cards were used for access control. But this **wasn't secure enough**. A person's card can be stolen and used to gain access to a restricted area. In some cases the card can be placed back without the person even realizing that it was stolen.

Some companies combined the cards with passwords in a bid to strengthen the security. But even these systems had flaws, **the biggest flaw being people**. Some people will lend out there card and password to friends or co-workers, without considering the consequences of their actions. Weaker passwords can be cracked and used with a stolen card.

This is where Smart Cards come in. Smart Cards can be **combined with biometrics for the best security**. The biometric template will be stored on the card where it is safe from tampering. A person's biometric identifier can't be imitated and is unique to that person. The biometric can't be stolen and or used without the knowledge of the person.

Another use of Smart Cards that can be classified as access control is in **satellite television decoders** (see [7]). The decoder needs a valid Smart Card before it will function and display the incoming signal.

The last Smart Card application that we will discuss in this chapter is for the use of travel and ticketing.

4.9 Travel and Ticketing

Tickets for **public transport** like trains and busses have to be bought before a person can make use of the transport (see [3]). Other card types are being used for these purposes, but Smart Cards will provide more options.

Smart Cards can then be used as throw away or disposable cards (but the price of a card is too much at the moment for this option) or as reusable cards. **Reusable cards will be the better option**.

Smart Cards will also offer better security against fraud and tampering of the data on the card, ensuring that only cards issued by the company can be used (see [3]).

The use of Smart Cards for **parking lot tickets** will yield the same result as for public transport. But this option will probably only be used by big companies with a special parking lot for their employees. At this point it will not be feasible to hand out a Smart Card to a once off visitor or user of the parking lot. This is the reason why malls won’t easily accept this system.

4.10 Summary

In this chapter we took a look at eight applications that Smart Cards can be used for. With each application we identified some areas where Smart Cards will be an improvement.

Smart Card applications are: payphone cards, SIM cards, financial cards, medical cards, social cards, loyalty cards, access control and travel and ticketing.

In these applications different advantages of Smart Cards are used to improve the application. For some it is the advanced security that Smart Cards offer, for others it is the storage space and processing power.

It doesn't matter what the reason is for using Smart Cards, they are a big improvement and their advantages are huge.

In the next chapter we will discuss some of the problems that may still exist in these Smart Card applications.

Chapter 5: Evaluating Smart Card Applications and their Short Comings

5.1 Introduction

Even though Smart Cards are a big improvement on its predecessors, in certain areas and in certain applications they can still fall short. The short comings can be anything from the price of the card and the system to problems with usability and constraints that may exist.

In this chapter we will take a look at the Smart Card applications of chapter 4 and discuss how Smart Cards are utilised and try to discover any short comings of the Smart Card in those applications.

5.2 Short Comings of a Smart Card in Applications

Smart Cards are faster, more secure, with processing power and more storage space. These are very important factors that contributed to the success of the Smart Card over any other card in all of the applications discussed in Chapter 4.

Even though Smart Cards are a big improvement, there are still a lot of problems that can arise when using these applications. Some of the problems are minor, and some come can be overcome, while others will have to be accepted.

The first problem of a Smart Card that we will discuss is wear and tear. This is only applicable to contact Smart Cards.

5.2.1 Wear and Tear

This problem exists for contact Smart Cards that will be used over a long period (see [10]). This can happen in all of the applications mentioned in Chapter 4 except for SIM cards. The gold plated chip makes contact with pins in the reader. As the card slides in and out of the reader the marks on the gold plated chip becomes worse.

Even though Smart Cards are a big improvement on other card technologies, they still have limited memory.

5.2.2 Limited Memory

The only application where a Smart Card doesn’t have enough memory would be the SIM card. As a cell phone has many applications to run and data to store, the Smart Card has insufficient memory to handle all of this. External memory (Micro SD and Mini SD cards) solves this problem.

The third problem that may arise in some Smart Card applications is the environment of use.

5.2.3 Environment

The environment can play a big role in the functioning of Smart Cards. Extreme temperatures can have a negative effect on the card, especially heat. Smart Cards have no way to cool down the micro processor, and extreme external heat can cause damage to the card or processor (see [4]).

This problem may exist where the system is installed, or where the card might be placed. A card left in the sun in a closed car might be damaged.

The following problem is only applicable to contact Smart Cards, and can be time consuming.

5.2.4 Throughput of Contact Smart Cards

Throughput is the amount of people that can pass through the system in a specific amount of time. Contact Smart Cards will take longer than contact less technology (see [10]). The person needs to insert the card and then wait to be authenticated. Combine this with biometrics and the throughput will be even worse.

Contact less cards will have a better throughput (see [3]). But biometrics will always slow down the process. A lower throughput will be the price for better security.

When new technology like biometrics is used, the users will need to go through training. This may pose a problem when the user base is too large to train.

5.2.5 Training Needed for Biometric Readers

When biometrics is combined with Smart Cards, for example in access control, the users will need training. Depending on the type of biometric used, users will have to be trained on how to use the reader and what not to do (see [19]).

Further more, some biometrics are seen as intrusive and not accepted by certain religions.

Smart Cards are a relatively new technology. This means that the cost of Smart Cards and the readers are still high. This brings us to the next problem that Smart Card applications can have.

5.2.6 Costs of Smart Cards

At this stage the cost of Smart Cards are too high to be used as disposable cards. We do have telephone cards that are disposable cards (see [10]). These cards are a type of Smart Card but not a true

Smart Card in every sense. They have less storage space and are not as powerful as a true Smart Card. This is why they are cheaper and can be used as a disposable card (See [7]).

One of the biggest problems with any system is the users. Users can be ignorant and spiteful. The last problem with Smart Card applications is the user.

5.2.7 People Using the Card

The biggest problem is always the user. It is the user that causes the damage to cards, or in access control environments will lend out his card to a co-worker. If people can be taught to be more responsible with their card, many problems can be neutralized.

Several problems can exist when using Smart Card technology, but these problems are not big enough to deter people and companies form using Smart Cards in their applications. The advantages of Smart Card technology are too huge to ignore.

5.3 Summary

This chapter concentrates on the short comings of Smart Cards in the applications that were discussed in chapter 4.

Problems with Smart Cards in these applications that have been identified are:

Wear and tear,
Limited memory in cell phones,
Environment of use,
Throughput time,
Cost of Smart Cards,
Training that is needed when Smart Cards are combined with biometrics, and

The biggest problem will be the people using the card.
These problems should be kept in mind when using Smart Cards but shouldn’t pose big problems for the applications.

The last chapter of the literature study is chapter 6, which will concentrate on fingerprint technology. This chapter is relative to the project as fingerprints will be combined with Smart Cards for a more secure access control application.

Chapter 6: Biometrics: Fingerprint

6.1 Introduction

Fingerprint identification is the most widely used biometric in the world today. It is easy to use, non intrusive and can be used for verification and identification of a person.

> **Identification**: the system can identify who the person is, a one to many match (see [19]).
> **Verification**: the system can only verify who the person is, a one to one match (see [19]).

The fingerprint scanner uses a silicone sensor to capture the fingerprint image and then process it into a template.

Figure 6.1: The fingerprint scanner on the ACS Smart Card reader

This chapter will take a look at how fingerprint biometrics work, looking at a few factors that will play a role when using this technology. Firstly we will start with the fingerprint itself.

6.2 The Fingerprint

The fingerprint has long been used for the identification of a person, especially in the criminal sector (see [20]). On a fingerprint you will find certain patterns and ridge flows that define the finger and make it unique (see [18]). These two aspects are divided into minutiae and patterns, and both can be used for matching (see [18]).

We will first take a look at the minutiae that can be found on a finger.

6.2.1 Minutiae

Minutiae are the ridge flows on your finger, more specifically what happens to the ridges (see [16, 18]). A minutiae point will be where a ridge ends or starts, where it splits (also called bifurcations) or where deltas are formed by these ridges (see figure 6.2).

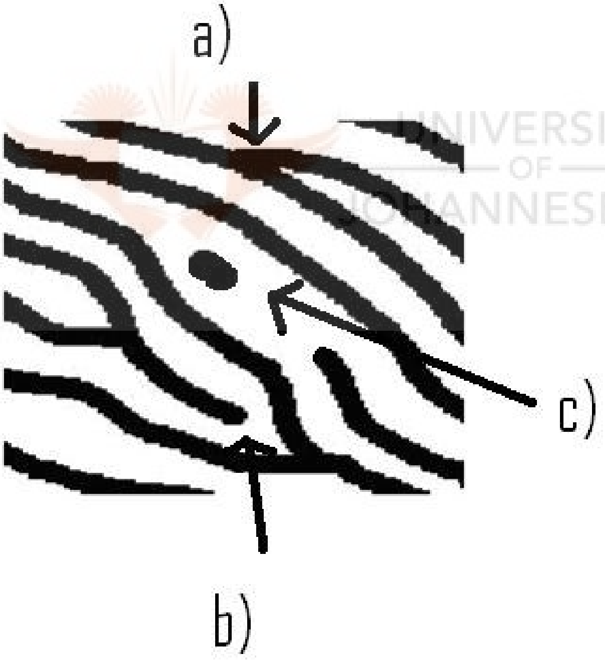


Figure 6.2: a) Bifurcation, b) Ridge Ending, c) Delta (see [37])

Ridges are the lines on the finger, and the ridges are separated from each other by valleys (see [16]).

On a single fingerprint there are about a 100 minutiae (see [16]). Most matching algorithms need only about 14 or 15 of these points to make a positive match. When capturing a fingerprint, only about 30 to 60 minutiae are captured to be used (see [16]). From this only 20 to 30 points are stored in the template when the storage space is limited, for instance Smart Cards.

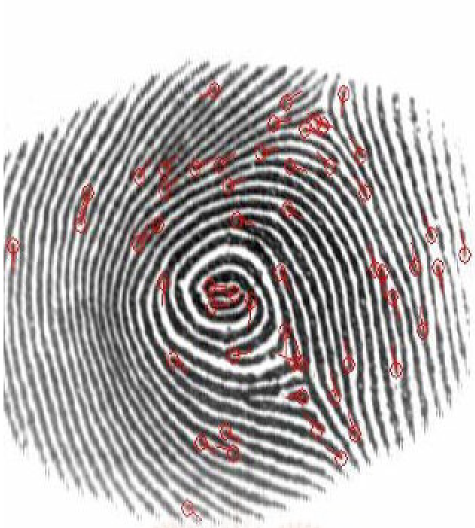


Figure 6.3: Minutiae points found on a finger for identification

Minutiae are used for the identification of a person and can deliver very good results.

We will now take a quick look at a few advantages and disadvantages of minutiae (see [18]).

6.2.1.1 Advantages of Minutiae

The first advantage of minutiae that we will look at is the identification of a person.

6.2.1.1.1 Identification

Minutiae based fingerprint matching can be used for identifying a person quickly against a large database, a one-to-many search (see [18]).

Minutiae matching have been used for many years now. It started as a manual process and was automated later on. This brings us to our next advantage of using minutiae. Minutiae are a well studied field.

6.2.1.1.2 Well Studied Field

Since this method has been used for many years a lot of research has been done in this field. More detail and information is available for future use (see [16], [18], [20]).

We will now take a look at the disadvantages of minutiae.

6.2.1.2 Disadvantages of Minutiae

The biggest disadvantage of minutiae is that it can be damaged.

6.2.1.2.1 Damaged Minutiae

Minutiae can be damaged by cuts and constant friction from a rough surface. With time minutiae can be changed permanently or even become missing from the finger because of friction (see [18]).

The second method that can be used for fingerprint matching is patterns. We will now discuss patterns.

6.2.2 Patterns

Patterns on the finger are also called the characteristics of the finger (see [18]). Three different types of patterns can be found (see [16]):

1. Loop: makes up about 65% of all patterns on the finger.
2. Whorl (Figure 6.4): makes up about 30% of the patterns found on a finger. The whorl is defined by at least one ridge that makes a full circle (see [16]).
3. Arch (Figure 6.5): has a more open curve than a loop.

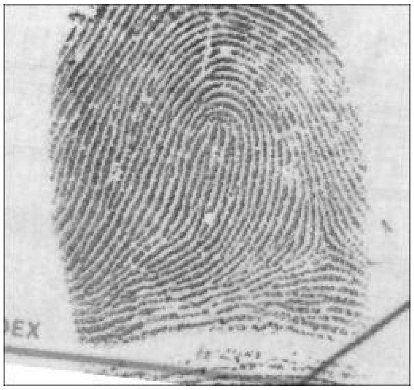


Figure 6.4: Whorl (centre of the finger) surrounded by a loop

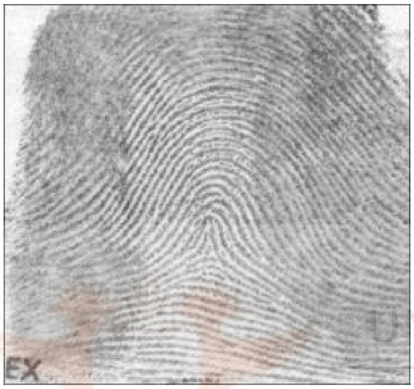


Figure 6.5: Arch on a fingerprint

Patterns also include detail like ridge thickness, curvature and the density (see [18]).

Three sections of the finger are captured when using this method. These sections are usually around some minutiae, but some cases exist where they are not. In some cases where minutiae are missing from the finger, pattern matching will still work.

We will now take a look at some advantages and disadvantages of using patterns for fingerprint matching (see [18]).

6.2.2.1 Advantages of Patterns

Pattern matching has three advantages. The first one that we will discuss is low resources needed for this algorithm.

6.2.2.1.1 Low Resources

Pattern matching is ideal for use with Smart Cards since they don't need many resources for the matching algorithm (see [18]).

The next advantage of pattern matching is a big problem for minutiae matching.

6.2.2.1.2 No Minutiae

This method will work even in the absence of minutiae (see [18]).

The last advantage of using patterns is that noise on the image won't affect the algorithm.

6.2.2.1.3 Bad Quality Image

The image quality won't affect the result as with minutiae based matching (see [18]).

We will now take a look at the disadvantages of this fingerprint matching algorithm.

6.2.2.2 Disadvantages of Patterns

The disadvantage of pattern matching is that it takes longer for identification of a fingerprint.

6.2.2.2.1 Not Optimized for Identification

Pattern matching will work very well for verification, no matter the size of the database (see [18]).

For identification it will take longer to find a match, and the time will increase as the database gets bigger. The results of correct matches may also decrease.

We have now looked at minutiae and pattern matching of fingerprints, their advantages and disadvantages. The next part about fingerprints that we will take a look at is the latent impression of a fingerprint.

6.2.3 Latent Impression

When a finger comes in contact with surfaces it leaves a fingerprint. This is called a latent impression. On certain surfaces, like glass the fingerprint will be visible. For the fingerprint to be visible on the glass, something needs to be left behind on the glass that defines the fingerprint.

This latent impression that a finger leaves on touched surfaces consists of (see [20]):

1. Perspiration,
2. Organic solids (amino acids),
3. Inorganic solids (blood and salts) and
4. Any other susceptible material that the finger might have been in contact with.

In a person's everyday actions his fingers comes in contact with dirt, oil and perspiration. These materials stay on the finger and are responsible for the latent impression.

The next section that we will discuss is the template creation and all the steps involved to capture the fingerprint.

6.2.4 The Template

This is where the captured fingerprint is stored in binary format (meaning 0's and 1's). Many Smart Cards today have limited storage space of between 8 and 32 Kbytes. This leaves us with only a little space for the template. A fingerprint template size can vary between 100 bytes and 1500 bytes (see [16]).

In some cases the finger is only enrolled once into the template, but it is better to enrol the finger more than once. This will improve the quality of the template and will yield better matching results (see [16]).

There are three levels of detail that is considered and used when capturing a fingerprint (see [20]). The three levels are:

1. The overall appearance of the finger, this includes the patterns, ridge flows and ridge count.
2. Friction ridge detail and path: this is the location of major changes in individual ridges.
3. The last one is individual ridge details. This includes dimensional attributes, shapes and width.

Each of these levels captures detail that will be used in the fingerprint template.

Creating and using a template involves a few steps (see [20]). These steps will now be discussed, starting with the acquisition of the image.

6.2.4.1. Acquire the Image

Acquire the fingerprint image from the fingerprint scanner. Remove all background from the image. This step also includes edge detection and a ridge flow algorithm (see [20]).

The second step in this template creation is to process the fingerprint.

6.2.4.2 Process the Fingerprint Region

This includes thinning the ridges to 1 pixel and then binarizing them (see [20]).

The third step to creating a template involves minutiae or patterns.

6.2.4.3 Find Minutiae or Patterns

This stage starts to find all the minutiae points of the finger or the patterns that the ridges form (see [20]).

After these three steps we can create our template.

6.2.4.4 Now a Template can be Created

Create the template and then store it in binary form. The size may differ, but most of the times it is about 1000 bytes (see [20]).

In the next two steps the template is used to match a fingerprint. The first of the two steps is to calculate a match score.

6.2.4.5 Calculate Match Score

Here the stored template and the newly captured template will be compared to calculate a match score. This match score will be a number that indicates how close the two fingerprints (templates) are to being the same finger (see [20]).

After the match score has been calculated, we apply a threshold value. This is the last step in creating and using a template.

6.2.4.6 Apply Threshold

The threshold is a value that determines what the match score should be to declare a positive match (see [20]).

Now that we have looked at the latent impression and the template of a fingerprint we can move on to the next section of fingerprints.

When using a biometric system like fingerprint matching, certain errors can occur. These errors can happen at the reader (incorrect use of the reader) or at the matching algorithm. When using fingerprint recognition certain errors and the rates at which they occur must be kept in mind. High rates will cause problems and be insufficient for use. Low rates are the ideal situation. Here are three important rates (see [23]):

6.2.5 False Rejection Rate (FRR)

This is also known as False Non-Match Rate or Type I Error. This is every time a valid (registered) finger is presented but then rejected as an invalid (unregistered) finger. No match could be found in the repository.

To calculate this we take the number of false rejections over the total number of samples (accepted and rejected) and multiply it by 100 (see [23]).

The second important rate of biometrics that we will look at is FAR.

6.2.6 False Acceptance Rate (FAR)

This is otherwise known as False Match Rate or Type II Error. This happens when a person presents an invalid (unregistered) finger and the prototype makes a match and lets the person in.

This is calculated by taking the number of false acceptances over the total number of samples (accepted and rejected) and multiply it by 100 (see [23]).

The third rate that should be kept in mind when using biometric systems is FTER.

6.2.7 Failure to Enrol Rate (FTER)

Failure to enrol is calculated by using the number of unsuccessful attempts to enrol over the number of attempts (successful and failed) (see [23]).

Possible causes for failure to enrol might be:

1. User inexperience with the technology,
2. The orientation and position of the finger might be incorrect,
3. The user might be moving his finger while a scan is made.

Fingerprint matching is very accurate. It has a very low Equal Error Rate (see [16]). A low Equal Error Rate means that the FAR and FRR are very low. This technology is also a lot cheaper than other biometric technologies. The fingerprint scanners will function correctly in a wider variety of environments than other biometrics, making them more robust. For increased accuracy and flexibility in a system multiple fingers of each user can be enrolled (see [16]). All of these factors played a role in fingerprint recognition becoming a widely accepted and used technology.

In the next section we will look at some problems with fingerprint technology. This includes attacks that can be launched on the system.

6.3 Problems with Fingerprint Technology

As with any good thing, there will always be a few problems. In this case most of the problems start with the people. Here are a few problems that may occur when using this technology. It is very important to keep this in mind when deciding on which biometric technology to use (see [15]).

The first problem of fingerprint recognition that we will look at is the distortion of the image.

6.3.1 Distortion of the Image

This can be due to elastic deformation. A distorted image will be difficult to read, process and then match. This can result in false matches or false rejections being made (see [15]).

The second problem with fingerprints has to do with the user's inability to use the technology correctly.

6.3.2 Incorrect Placement of Finger

Sometimes only a partial image of the finger might be captured because of incorrect placement. Other problems that there might be are (see [20]):

1. The rotation of the finger compared to the scanner can differ,
2. Differences in pressure will move the minutiae closer or further away from each other,
3. The orientation of the finger to the scanner might be different.

The next problem that we will look at will only be a problem with minutiae matching and not pattern matching.

6.3.3 Missing Minutiae

Minutiae might be missing from certain people due to a lot of friction of the fingers. Furthermore, minutiae can be damaged by cuts, changing them forever. A lot of dirt, moisture or humidity will have a big effect on the quality of the image (see [20]).

The fourth problem with biometric systems is that users may have a malicious intent.

6.3.4 Malicious Users

These users may want to avoid recognition by the system for several reasons (see [15]).

One fact that will remain is that a person can't reproduce the exact input image of another person (see [17]). There are however several ways to try and do this. These are seen as attacks on the system.

Attacks are the fifth problem with fingerprint technology that we will discuss.

6.3.5 Attacks

There are several attacks that a user can try on a system to break through or bypass the security. We will discuss four types of attacks: trail and error, replication, theft and digital spoofing (see [19]). We will start by looking at trail and error attacks.

6.3.5.1 Trail and Error Attacks

This section has two types of attacks: password guessing and biometric team attacks (see [19]). Password guessing will only play a role when biometrics is combined with passwords. For the Smart Card VeriSys we didn't use passwords, but in the future there might be a need to use passwords combined with Smart Cards and biometrics.

6.3.5.1.1 Password Guessing

This is usually an offline attack where the perpetrator tries to crack the password (see [19]). A dictionary attack is used in some cases. This is successful because a lot of people use words that can be found in a dictionary for a password. This method works against weak passwords.

6.3.5.1.1.1 Weak Password

This is usually a short (4 or 5 characters), lower case word or name of a family member.

Weak passwords make trail and error attacks easier, which is a big problem for any security system.

6.3.5.1.1.2 Strong Password

The password is at least 6-8 characters long, lower and upper case characters. The password must also consist of alphabetical, numerical and special characters.

A new trend is to refer to a pass phrase and not password. A strong pass phrase won't be a dictionary word or name, but rather random characters or a sentence. It is very difficult to crack a strong password or pass phrase by using password guessing.

The second type of trail and error attack that we will discuss is biometric team attacks.

6.3.5.1.2 Biometric Team Attacks

The person takes a group of people with him and tries to get access through a positive match from a person in the group (see [19]). No one of the group will be registered in the system. Theoretically a big enough group might get a match. The system should detect all the failed attempts and block them.

The second type of attack that a person can try on a biometric system is replication of the biometric (see [19]).

6.3.5.2 Replication

A copy of the biometric is made and this fake biometric is then presented to the biometric scanner. A copy of a fingerprint can be made using the gelatine (gummy bear) finger method (discussed in Chapter 9). It is a lot harder to spoof biometric systems than it sounds, and harder than Hollywood makes it out to be. Certain biometrics can only be read with your knowledge, so they can't be stolen without you being part of the scam.

In the case of fingerprints that are left on a lot of places, it is not that easy to retrieve and reproduce a finger that is precisely the same. This method will fail when liveness testing is done with the biometric. For example, the copied finger won't have the same heat signature as a live finger.

The fifth problem with fingerprint technology is attacks on the system. The first two types of attacks are trail and error attacks and replication. Next we will discuss the third type of attack, theft (see [19]).

6.3.5.3 Theft

The beauty of biometrics is that it isn't easy to steal a person's biometric without his knowledge. It is part of your body, and you can't forget it. Stealing the biometric isn't easy, but it isn't impossible. In most cases the electronic version of the biometric will be stolen when the biometric is send over a network (see [19]).

The last attack that we will look at is digital spoofing (see [19]).

6.3.5.4 Digital Spoofing

This method relies on the fact that in many systems the newly captured fingerprint needs to be sent over a wire (network) to be authenticated (see [19]). The fingerprint (the template) will be send as bits over this network. The attacker then sends his template, which he either stole or created himself, and tries to get in.

This attack shows us how important it is to protect the databases against attacks and illegal entry. An unsecured database can be hacked and templates can be stolen (see [19]).

The next section doesn't cover problems with fingerprint technology, but rather defences against attacks on the system. Attacks are a big problem and these defences are quite important for a save and secure system.

6.3.6 Defences

It is important for a system to be able to resist attacks. There are several methods to do this. We will now take a look at a few ways to increase the security of the system.

First we will discuss defences against trail and error attacks (see [19]).

6.3.6.1 Trail and Error

Increase the base secret. The base secret is the measured property of your biometric. A bigger base secret will make it harder to crack (see [19]).

Another method is to only allow a person three chances of providing the correct biometric.

The next defence that we will look at is against replication of the biometric property.

6.3.6.2 Replication

The best defence here would be to test for the liveness of the presented biometric (see [19]). Some biometrics has heat signatures, others will have a pulse or a reaction of some sort (discussed in Chapter 6.4). A copied (fake) biometric will not pass the liveness test.

The third defence is against theft (see [19]).

6.3.6.3 Theft

Combining biometrics with pins or passwords will make it useless for someone to steal the biometric (see [19]).

Attacks on a biometric system can have many forms. We have now looked at trail and error attacks, replication and theft. The last type of defence against attacks that we will look at is digital spoofing (see [19]).

6.3.6.4 Digital Spoofing

Here a simple challenge response will be sufficient. This method is used a lot on the internet when signing up for newsletters or registering to a web site. This will make sure that it is a real person making the request and not a machine.

Biometric systems can be attacked using many different methods, but fingerprints in particular are vulnerable to two types of attacks (see [20]):

1. Masking the finger to avoid a match. In this case a person can then blame the system for his absence from work.
2. Spoofing the device in a hope to force a false match. The person will hope to get entry to a secured area or to secure data.

We have now looked at some problems with biometric systems, attacks on the system and defences against some of these attacks. We will now expand on one of the defences against attacks. The next section of biometric fingerprint technology that we will discuss is liveness testing.

6.4 Liveness Testing

Biometric systems can be spoofed using fake and reproduced biometric identifiers. Another element is needed to make sure that the system is not spoofed. This is where liveness testing comes in. Liveness testing is used to make sure the presented biometric is still a valid, original and living human body part (see [21]).

Liveness testing is divided into three parts: intrinsic properties of the human body, involuntary signals generated by the body and responses to a stimulus (see [21]). Depending on the biometric used the type of tests may differ.

We will start by looking at the intrinsic properties of a human body (see [21]).

6.4.1 Intrinsic Properties of a Human Body

Living as well as dead bodies will have some of these properties, but biometric copies and instruments used for spoofing may lack these properties (see [21]). Intrinsic properties of the body can be:

6.4.1.1 Physical or Mechanical

This includes weight, density and elasticity (see [21]).

6.4.1.2 Electrical

This is capacitance, resistance, impedance and dielectric constant (see [21]).

6.4.1.3 Visual

This includes the appearance and the shape of the biometric. Other visual elements are opacity and the colour (see [21]).

6.4.1.4 Spectral

Transmittance, absorbance, reflectance and fluorescence are all spectral elements (see [21]).

The last intrinsic property of the human body that we will discuss is body fluid.

6.4.1.5 Body Fluid

Elements include oxygen, blood, DNA and constituents (see [21]).

The second part of liveness testing is involuntary signals of a body (see [21]). This is the second group of properties that can be used by biometric readers for liveness testing.

6.4.2 Involuntary Signal Generated by the Body

These signals will always be present in a living body. They are produced by the body itself and can not be imitated or reproduced (see [21]). This includes (see [21]):

1. Pulse,
2. Blood pressure,
3. Heat,
4. Thermal Gradients,
5. Transpiration of gasses,
6. Body odour and
7. Brain wave signals (EEG).

The last group of properties of a body that can be used for liveness testing is the response to a stimulus (see [21]).

6.4.3 Responses to a Stimulus

This is a reaction (voluntary or involuntary) to some action that has happened (see [21]).

We will start by looking at voluntary responses.

6.4.3.1 Voluntary (Behavioural) Response

The user is asked to perform a task as a response. The stimulus can be divided into three categories (see [21]):

1. Tactile: The user will feel something,
2. Visual: The user will be shown something, or
3. Auditory: The user will hear something.

The second type of response to a stimulus that we will discuss is the involuntary response.

6.4.3.2 Involuntary (Reflexes) Response

In this case the user doesn't really have the option to respond or not, his body will automatically respond. The stimulus can be (see [21]):

1. Electromyography (EMG),
2. Pupil dilation, or
3. Reflex of a knee when struck.

Fingerprint technology uses intrinsic properties of a body. It measures the index of refraction, capacitance and the acoustic impedance of the finger (see [21]).

Liveness testing can be strong or weak. It depends on the biometric property (see [21]). In the next section we take a look at when liveness tests are weak and when they are strong.

6.4.4 Weak and Strong Liveness Tests

Liveness testing can be weak or strong. A weak liveness test is an extra test that should be done while reading the biometric (see [21]).

Strong liveness tests are done at the same time when the biometric is read (see [21]). Actually, when a biometric can only be read from a living body, it will also be a strong liveness test (see [21]). An example of this is a facial thermograph: body heat (in that specific pattern) will only exist in a living body, so there is no need for further liveness test.

This means that fingerprints will use weak liveness testing, and requires a separate test to check for liveness.

There are a few methods to help improve liveness testing or just to supplement them. A point that should be remembered is that when a system is made by man, it can be defeated by man (see [21]). It is better to be safe and have a secure system.

1. Combine the biometric with a pin or password,
2. Combine the biometric with something that the user have (like a Smart Card), or
3. The best and safest way is to combine biometrics with a pin or password and with something that the user has (see [21]).

We have now discussed fingerprint technology in general, the problems with fingerprint technology and liveness testing of biometric properties. Next we will take a look at some standards for fingerprint technology.

6.5 Fingerprint Standards

In this section we will take a quick look at two of the leading standards for fingerprints (and biometrics) combined with Smart Cards. The two standards that we will look at are ISO 7816 part 11 and BioAPI.

We will start with ISO 7816 part 11.

6.5.1 ISO 7816 part 11

The first three parts of this ISO 7816 standard covers Smart Card specifications and were discussed in chapter 2.5. Part 11 is Personal verification through biometric methods (see [18]).

This standard specifies inter industry commands and data objects for personal verification using biometrics combined with Smart Cards.

Examples of enrolment and verification of the biometric property and security issues are also included in this standard.

The next standard that we will discuss is BioAPI (see [22]).

6.5.2 BioAPI

The Biometric Application Programming Interface (BioAPI, see [33]) is a standard that regulates the enrolment and verification of biometric properties in a system. BioAPI allows the integration of modules from different vendors to produce a working system. BioAPI define interfaces for these modules to make integration easier (see [22]).

Integrated modules can be software components, fingerprint scanners, modules for image processing or modules for matching and searching.

6.6 Summary

This was the last chapter of the literature study and concentrated on fingerprints as a biometric property for identification.

We started off by looking at fingerprints in general. There are two methods to use fingerprints for identification and verification. The first uses minutiae. That is ridge endings, deltas and bifurcations that are formed by the ridges on the finger. The second method uses patterns that can be found on the finger. There are three patterns: loops, whorls and arches.

From this chapter it became clear that minutiae matching are well suited for identification of a person, whereas pattern matching is not optimized for identification. Pattern matching will be the fastest at verification of a person.

Three important rates to keep in mind when using a biometric system are the Failure to Enrol Rate (FTER), False Acceptance Rate (FAR) and the False Rejection Rate (FRR).

Several problems may arise when using biometrics. Problems that may be encountered when using fingerprints are:

Distortion of the image,
Incorrect placement of the finger,
Missing minutiae,
Malicious users and
Attacks on the system.

Attacks pose the biggest problem for the security of the system. Four types of attacks that can be launched against the system are: trail and error, replication, theft and digital spoofing.

There are defences that can be used against each of these attacks, but the best defence is liveness testing. Liveness testing is used to check that the presented biometric is a living biometric. The three types of liveness testing are: test for intrinsic properties of a human body, test for involuntary signals of the body and the test for responses to a stimulus.

Two of the biggest standards for biometrics combined with Smart Cards are ISO 7816 part 11 and BioAPI.

This was the last chapter of the literature study. In the next chapter we will look at the Smart Card VeriSys prototype system.

Chapter 7: Smart Card VeriSys: A High Level Description

7.1 Introduction

The prototype will be a simple working system that will show the use of a Smart Card combined with fingerprints for access control at a University. The card will be used as a student card.

In this chapter we will look at the system. We will explain how the system works and discuss the authentication process.

7.2 Smart Card VeriSys

The Smart Card VeriSys prototype consists of two parts: Registration and Authentication.

7.2.1 Registration

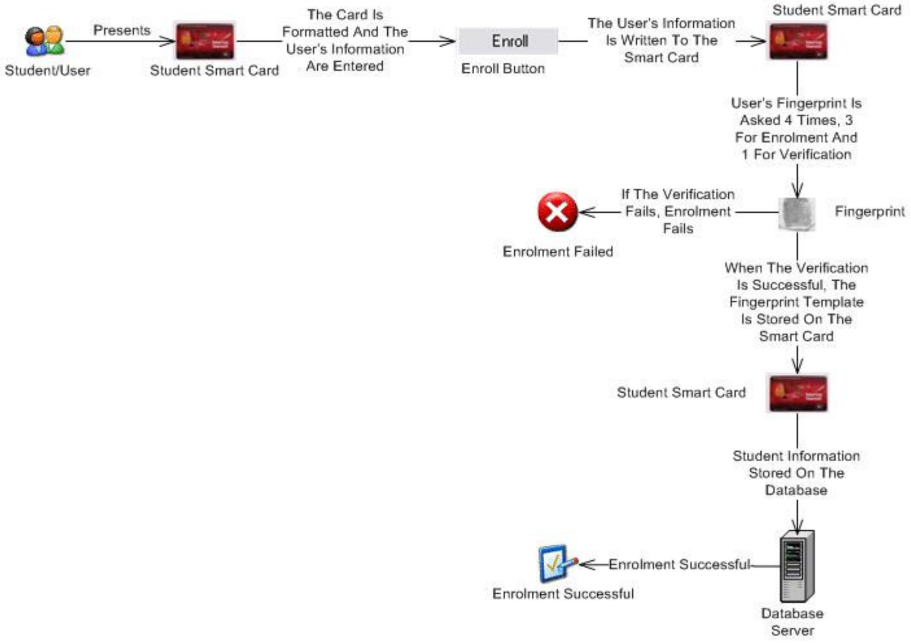

Student/User
Presents
Student Smart Card
The Card Is Formatted And The User's Information Are Entered
Enroll
Enroll Button
The User's Information Is Written To The Smart Card
Student Smart Card
User's Fingerprint Is Asked 4 Times, 3 For Enrolment And 1 For Verification
Fingerprint
If The Verification Fails, Enrolment Fails
Enrolment Failed
When The Verification Is Successful, The Fingerprint Template Is Stored On The Smart Card
Student Smart Card
Student Information Stored On The Database
Database Server
Enrolment Successful
Enrolment Successful

Figure 7.1: Smart Card VeriSys Registration Process

This part of the Smart Card VeriSys allows the user to register on the system. When the user's card is inserted into the reader, the card must be formatted to create the necessary files for data storage. Next we insert the user's information into the provided text boxes. Now we can enrol the user to the system.

The user's information will first be stored on the Smart Card. The user will be asked for his fingerprint a total of four times. The first three fingerprints are used to create the fingerprint template. Immediately after the template is created the finger will be verified using the fourth presented fingerprint, if this is successful, the template will be stored on the Smart Card. Now the user will be registered in the central database. If the fingerprint verification fails, registration will fail.

Authentication is the second part of the Smart Card VeriSys.

7.2.2 Authentication

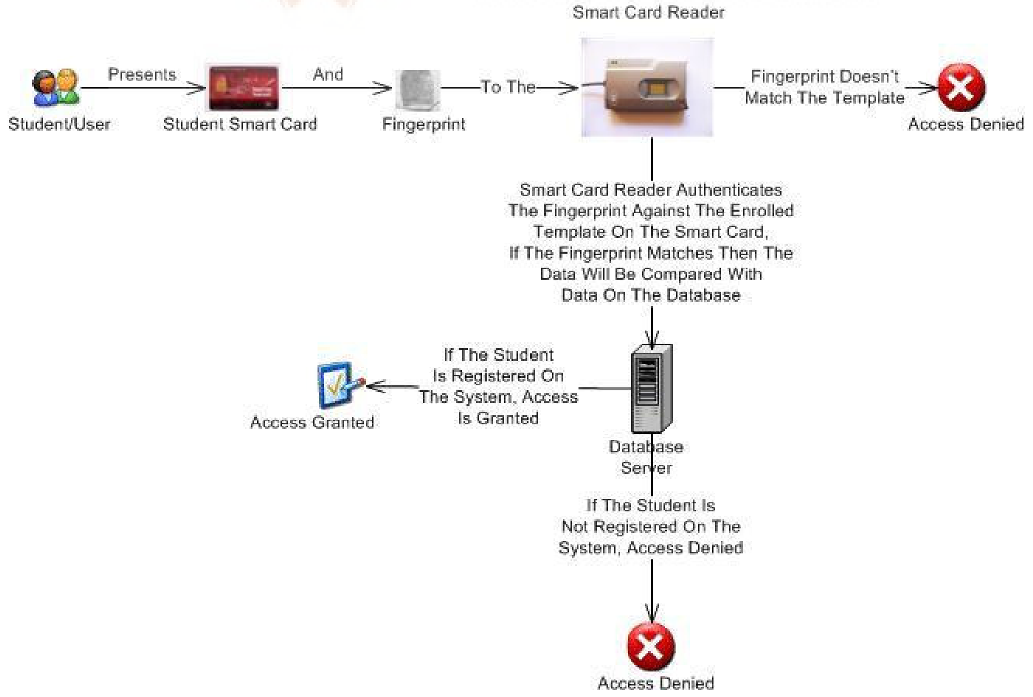

Smart Card Reader
Presents
And
To The
Fingerprint Doesn't Match The Template
Student/User
Student Smart Card
Fingerprint
Access Denied
Smart Card Reader Authenticates The Fingerprint Against The Enrolled Template On The Smart Card, If The Fingerprint Matches Then The Data Will Be Compared With Data On The Database
If The Student Is Registered On The System, Access Is Granted
Access Granted
Database Server
If The Student Is Not Registered On The System, Access Denied
Access Denied

Figure 7.2: Smart Card VeriSys Online Authentication

The user will insert his card into the Smart Card reader. The reader will connect to the Smart Card and retrieve the user's information. The user will be asked for his fingerprint. The fingerprint will be compared to the enrolment template and when the two match, the user's information on the Smart Card will be compared to the information in the database. If the user is registered in the database, he will be granted access. If the user is not registered in the database, access will be denied.

Next we look at some information about the Smart Card.

7.2.3 Smart Card

When the Smart Card is used for the first time it needs to be formatted. The format process creates the files on the Smart Card for the data to be stored in. This process is very important. The first five records on the Smart Card are reserved for the fingerprint template. The records after that are used to store the user's information.

When a card is not formatted, that is the files for data storage is not created and not the right sizes, the data can't be stored on the card.

For the prototype we created files for the fingerprint template, and then for the persons' name, surname, student number and ID number.

Before we create these files or change data in them we need to submit the Issuer Code (IC). This code restricts access to the files and the data. The IC is a secret code that the Smart Card VeriSys submits to the Smart Card when the card is formatted or data written onto the card.

The hardware used for the Smart Card VeriSys is a Smart Card reader and ten Smart Cards from Advanced Card Systems. More detail on this and the computer is provided in chapter 8.

7.3 Summary

This chapter explained how the two parts of the Smart Card VeriSys prototype works. The two parts are Registration and Authentication.

We also looked at the Smart Card and the actions that need to be performed for the Smart Card to function correctly.

Authentication for the Smart Card VeriSys is an online process. We need a connection to the database. This connection is used to compare the user’s information on the Smart Card to the information in the database. If there is a match the user will be granted access.

Smart Cards can be used for offline authentication. Offline authentication wasn’t implemented in the Smart Card VeriSys. When authentication is offline, no connection to an external computer or database is needed. The user will insert his Smart Card into the Smart Card reader and present his fingerprint. When the presented fingerprint matches the fingerprint template on the Smart Card, he will be granted access. All the processing is done by the Smart Card and the Smart Card reader. No computer is needed.

When using offline authentication a small program has to be stored on the Smart Card. When the Smart Card is inserted into the Smart Card reader this program will be executed and will give the necessary instructions to the Smart Card reader and fingerprint scanner.

In the next section we will take a look at the hardware and software that we used when building the Smart Card VeriSys.

Chapter 8: Hardware and Software used for the Smart Card VeriSys

8.1 Introduction

This chapter will concentrate on the hardware used for this prototype system. We will in particular focus on the Smart Cards, the Smart Card reader and the computer used.

We will look at some technical specifications for the hardware and some of their advantages.

We start by looking at the Smart Cards and the reader that we used for the Smart Card VeriSys.

8.2 Smart Cards and Reader

The Smart Card reader that we use is the AET 63 BioTRUSTKey from Advanced Card Systems (ACS). The Smart Card reader is combined with a fingerprint scanner to provide fast and secure capturing and verification of the fingerprint.

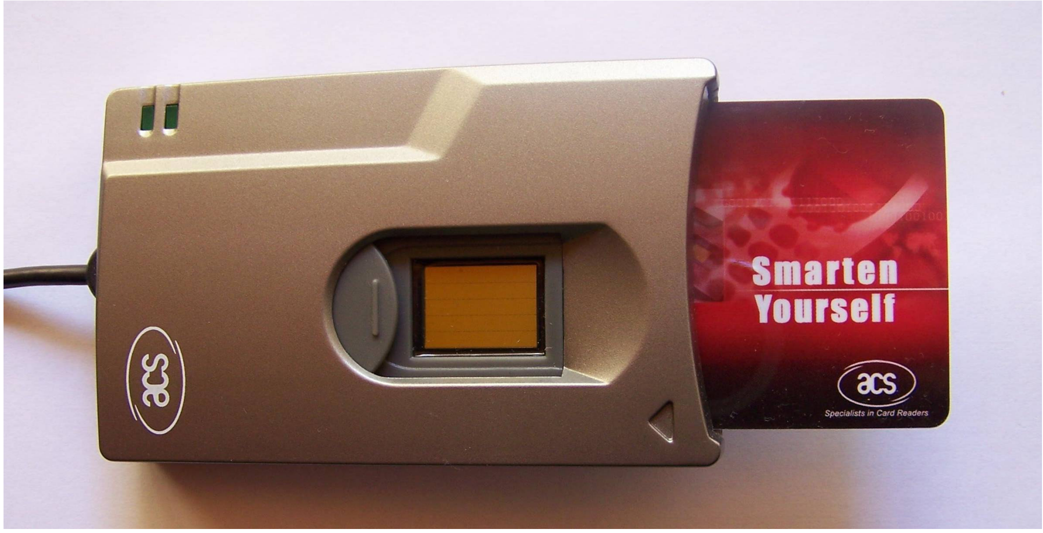


Figure 8.1: The ACS Smart Card reader with a Smart Card

Fingerprint template extraction and the matching algorithms are all dealt with inside the card reader. No data has to go to a pc (see [6]).

The reader uses USB (Universal Serial Bus) to connect to a computer. The speed between the card reader and the computer is 1.5 Mbps. Read write speed to a Smart Card varies between 9600 – 96000 bps (see [6]).

The fingerprint scanner is a silicon-based capacitive sensor that captures the image. Capacitive sensing is the most widely used technology for capturing fingerprints (see [16]). The advantage of using capacitive technology is that a real fingerprint is required to be picked up by the capacitive sensors (see [16]).

For detailed technical specifications of the ACS AET63 BioTRUSTKey see [6].

In the next section we will take a look at the computer used for the programming.

8.3 Computer

The computer that is used for this project is a personal computer with the following components:

Operating System: Microsoft Windows XP Professional
Version: 5.1.2600 Service Pack 2 Build 2600

System Manufacturer: INTEL
System Type: X86-based PC
Processor: x86 Family 15 Model 4 Stepping 1 Genuine Intel, 2802 MHz

Total Physical Memory: 1,024.00 MB DDR2
Total Virtual Memory: 2.00 GB

Hard Drive Description: Local Fixed Disk
Compressed:No
File System: NTFS
Size: 200.00 GB Serial ATA

In the next section we look at the software used to build the Smart Card VeriSys.

8.4 Software

Visual Studio .Net 2003 was used for the programming. The biggest part of the program is written in C#. The rest of the program is written in VC++.

To communicate with the Smart Card reader we used an API (dll file) provided by Advanced Card Systems. For us to use this API we needed to use a language like VC++ as C# was unable to use this dll file. In VC++ we created our own dll file that will communicate with the provided API, and C# is able to use our new VC++ dll file.

The database used for this prototype is MySQL Server 5.0 with SQLyog as the Graphical User Interface (GUI). The database name is **smartcard** and the table in the database is **main**.

The Smart Card VeriSys has about 8800 lines of source code. About 150 of these lines were written in VC++ to create our own dll file. The rest of the source code is written in C#.

The programming for Smart Card VeriSys started at the end of February 2007 and ended in middle August 2007. During this time a lot of work was done on the dissertation, not all the time was spent on programming.

Several problems occurred while writing the Smart Card VeriSys. The first real problem was to use the tfm.dll file. The tfm.dll is the Trusted Fingerprint Module file which is the application programming interface (API) that should be used to communicate with the fingerprint scanner. To use the tfm.dll we needed to use a language like C++ or VB6, and not C#. A big part of the program was already written in C# and it would take too long to change over to another language at this point. The solution to this problem was to use VC++. In VC++ we would create our own dll file (Finger_Module) that would use the tfm.dll. From C# we call the Finger_Module.dll which in turn calls the tfm.dll.

The next big problem that occurred while writing the Smart Card VeriSys was to store the fingerprint on the Smart Card. The tfm.dll provides us with functions to capture and store the fingerprint on the Smart Card, but from this function we got an invalid parameter error. Several other parameters were tested but got the same error. An email to Advanced Card Systems (info@acs.com.hk) resulted in help from Chiqui Acedilla (chiqui.acedilla@acs.com.hk). The solution is that the fingerprint must be stored in the first files on a Smart Card. When formatting the Smart Card we need to create 5 files where the fingerprint template can be stored and they must be the first files on the Smart Card. All the other information can be stored after that.

8.5 Security Settings

There are two security settings that we can change for the Smart Card VeriSys. These settings are: security levels for template matching and anti-spoofing security levels.

8.5.1 Security Levels for Template Matching

There are 5 security levels that we can use for this security setting.

Level 1: minimal security level

Level 2: low security level

Level 3: medium security level

Level 4: high security level, and

Level 5: maximum security level

The Smart Card VeriSys will use level 5 security, providing us with the best security for template matching. This high setting will help to avoid False Acceptances but might raise the False Rejection Rate.

Next we will look at the second security setting for Smart Card VeriSys: Anti-spoofing security.

8.5.2 Anti-spoofing Security Settings

For anti-spoofing there are 3 levels of security.

Level 0: none, no anti-spoofing tests

Level 1: standard, simple finger detect settings

Level 2: max, full anti-spoofing with individual anti-spoofing info stored in the fingerprint template

We use level 2 anti-spoofing for the Smart Card VeriSys, providing us with the best security against spoofing attacks on the system.

8.6 Summary

The Smart Card reader is an Advanced Card Systems product that combines Smart Cards and fingerprint technology. The fingerprint extraction and matching is handled by the reader, this provides a secure application. The Smart Card reader that is used is the AET63 BioTRUSTKey.

The computer that was used to build this application is a 64bit Intel machine running Windows XP with SP2. This computer will be used to test the program, which is why the components that are in the computer are so important. Different test results, especially when time is a factor, may be achieved using a different computer.

The programming languages used is C# and VC++ form Visual Studio .Net 2003. The MySQL database is an open source database.

We have now had a look at the hardware that will be used for the Smart Card VeriSys. In the next section we look at the test results.

Chapter 9: Testing the Smart Card VeriSys

9.1 Introduction

Testing a new program is very important. These tests should be devised to show us any deficiencies that might exist in the program. We want to discover any errors and failures.

Some of the tests are designed to show us the capabilities of this program. One of the most important tests will be the throughput (amount of people that can pass through the system in a time unit) that the system can handle.

In this chapter we will look at the types of tests that we performed on the system and mention a few extra tests that can be used. We will give the results of these tests.

In the next section we will discuss the tests that we performed on the system.

9.2 Types of Tests

Several tests were conducted on the system, testing as many as possible aspects of the system. Performance, security and dependability are really important.

We will start with the success rate of the fingerprint scanner.

9.2.1 Fingerprint Match Decision Accuracy

This test is done on the system to see what the False Acceptance Rates and False Rejection Rates are.

9.2.1.1 False Acceptance Rate (FAR)

This is when a match is made but the person is not enrolled on the system.

9.2.1.2 False Rejection Rate (FRR)

A person is enrolled on the system, but no match is made.

The idea is to keep both rates as low as possible, meaning that every match is an accurate match. With one-to-one verification it will be easier to keep these rates low.

This test will be performed on people that are enrolled to the system. For FAR and FRR tests, we will enrol clean and oily fingerprints and then do the authentication tests. These tests will be performed with clean fingers, oily fingers and dirty fingers.

For FAR people can exchange their cards and use different finger placements to see if they can force a match. Fake fingers will be used to try and spoof the fingerprint scanner.

Two types of fake fingers will be used to see if we can spoof the fingerprint scanner.

9.2.1.3 Wax Fingers

Modelling clay or prestik is used to make a mould. The finger is pressed into the prestik or modelling clay to form a finger with the fingerprints visible on the mould.

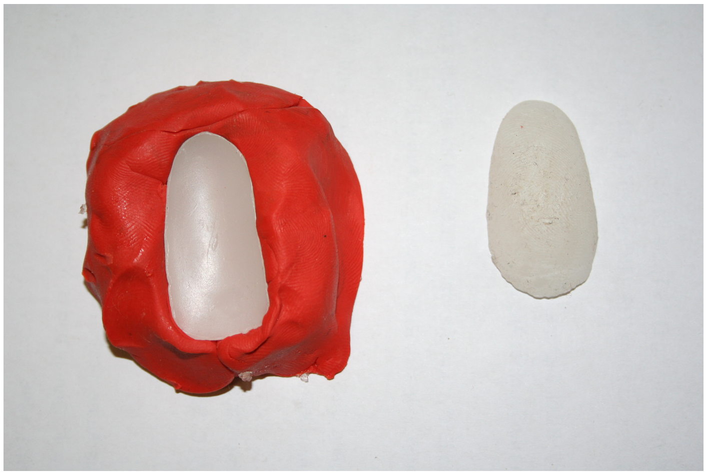


Figure 9.1: Wax Finger in mould and Wax Finger

Candle wax are then melted and poured into the mould. This is then placed in a freezer for about ten to fifteen minutes so that the wax can harden. When the mould is removed we have a fake finger.

9.2.1.4 Gelatine “Gummy Bear” Fingers

A mould is made from modelling clay or prestik. Press the finger into the mould, this will form a finger impression with fingerprints.

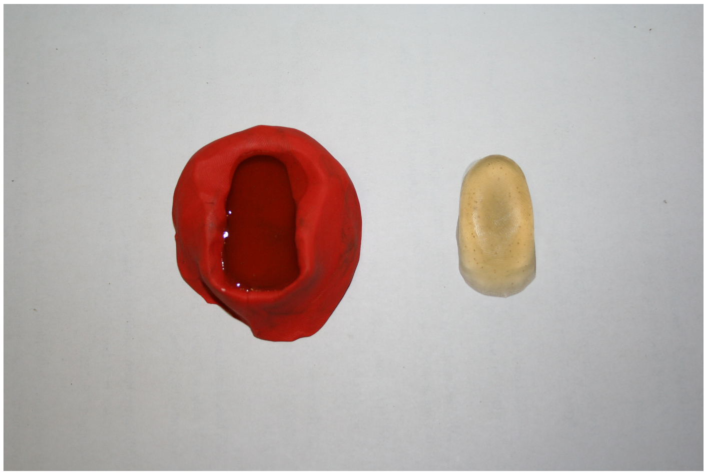


Figure 9.2: Gelatine Finger in mould and Gelatine Finger

Liquid gelatine is poured into the mould, this is then placed in a fridge to set. Remove the modelling clay or prestik and we have a fake finger.

The results and effectiveness of these two tests will be discussed in Chapter 9.3.

The second test that we will perform on the system is the failure to enrol a person at registration.

9.2.2 Failure to Enrol Rate

This test will check the failure rate when people register (enrol) to the system. This test will be performed during the registration process.

Several errors may occur, ranging from incorrect finger placement to an error with the Smart Card.

Tests will be performed with clean fingers, oily fingers and by untrained people using fingerprint scanners for the first time.

The next test is specifically for fingerprints: the failure of the scanner to acquire a fingerprint.

9.2.3 Failure to Acquire Rate

In this test we will check the failure to acquire a fingerprint from the scanner. This test will be performed on both the programs, enrolment and authentication.

The failure can be caused by incorrect placement from inexperienced users or a dirty scanner lens.

This test will explore the effect of clean fingers, oily fingers and dirty fingers on a fingerprint scanner.

The fourth test that we will look at is the rate at which users have to perform multiple attempts to authenticate themselves.

9.2.4 Multiple Attempt Error Rates

When authentication fails, a person will have to try again to gain access. This test is aimed at identifying the rate at which people have to make multiple attempts.

The test will be performed on the authentication program. Failures can be caused by the fingerprint or the Smart Card.

The test will be performed with clean, oily and dirty fingers. A person only has three chances for authentication.

The next test is an important test for any access control system, especially when it is combined with biometrics.

9.2.5 User Throughput

This test will measure the amount of people that can pass through a system in a certain amount of time.

We will perform this test on the authentication program, trying to get as many people as possible through the system in the specified time.

Ten cards will be used in the test, measuring each attempt’s time and the total amount of time. This will give us the average time that it will take a person for authentication.

There are a few other tests that can be performed on the system but were not seen as necessary. These tests include Matching Algorithm Throughput and time differences in using DES or Triple DES for encryption. The time difference between online and offline authentication can also be investigated. Online authentication uses the database to check that students are registered. Offline authentication does not connect to the database. The presented fingerprint will be compared to the fingerprint template on the Smart Card and if they match the user will be granted access.

9.3 Results

The results of the test will be given in this section. A discussion and evaluation of the results will be done in Chapter 12. We will start by looking at the match decision accuracy results of our system.

9.3.1 Fingerprint Match Decision Accuracy

The first test results that we will look at are that of False Rejection Rates (FAR). The ideal is to keep this rate as low as possible.

9.3.1.1 False Acceptance Rate (FAR)

The Smart Card VeriSys operates at the highest possible security levels, but for the FAR tests we lowered the security levels to the lowest security level possible for the Smart Card VeriSys. The security level for template matching is now Level 1 (minimum security level), and the anti-spoofing security level is now Level 0 (no anti-spoofing tests).

The first FAR test was different finger placements.

9.3.1.1.1 Test 1: Finger Placement

In this test on the system we used 9 Smart Cards that were already enrolled into the system. Ten fingers were used with different placements, with one finger (the one enrolled on the Smart Card) not being used. Each finger was tried three times.

With the different finger placements we tried to see if we can force a false match. As can be seen from the table, we had a total of 243 attempts at forcing a false match. All 243 attempts failed giving us a 0% FAR.

Attempts: 243	Failed: 243	FAR: 0%

The result was exactly what we hoped for.

The second test we explored the effect that oil based substances would have on forcing a false match.

9.3.1.1.2 Test 2: Oily Fingers

This test used the same setup as test 1, 9 Smart Cards, 10 fingers producing a total of 243 attempts.

In this case a lot of hand cream was used on the fingers making them extremely oily which would make the scanner dirty (leaving oily fingerprints on the scanner).

Attempts: 243	Failed: 243	FAR: 0%

These tests yielded the same result as test 1, with all 243 attempts failing to force a match. This gives us a 0% FAR, and that is what we are looking for.

The third FAR test we used dirt on the fingertips to try and make the fingerprint look a bit different to the scanner.

9.3.1.1.3 Test 3: Dirty Fingers

This test used the same setup as the two previous tests, 9 Smart Cards and 10 fingers. We used a lot of soil to try and make the fingerprint a bit different.

Attempts: 243	Failed: 243	FAR: 0%

The results once again proved to be the same as the first two tests. These gave us a total of 243 attempts and there where no false matches made. Another FAR of 0%.

At this point it was obvious for us to be able to spoof the scanner we needed a better method. First we tried wax fingers as discussed in section 9.2.1.3. After several attempts we had no luck of the scanner picking up the wax finger. No image could be captured. The reason for this could be the fact that the wax finger is hard and won’t have the same characteristics as a normal finger.

Next we tried gummy bear fingers as discussed in section 9.2.1.4. Three fingers where made from gelatine, a thumb, an index finger and a middle finger. Enrolment and verification tests were done with these gelatine fingers. The first of these are verification of the thumb.

9.3.1.1.4 Test 4: Gelatine Thumb Verification

A Smart Card that is enrolled with the original thumb print is used. The gummy bear finger is then used to try and force a match. This will be a false match.

Attempts: 20	Image Captured: 12
No Image: 8	FAR: 0%

As we can see from the table, 20 attempts were made to force a match. In only 12 of those attempts could the scanner pick up an image, but no match could be made. In the other 8 attempts the scanner couldn't get a big enough finger for an image or couldn't get a finger at all.

The gelatine thumb had a 60% image capture rate with no false matches.

The first gelatine finger gets a FAR of 0% which is a good result.

The next test was done with the gelatine index finger.

9.3.1.1.5 Test 5: Gelatine Index Finger Verification

This time a Smart Card enrolled with the original index finger was used for the test.

Attempts: 20	Image Captured: 16
No Image: 4	FAR: 0%

From the 20 attempts, the scanner was able to capture 16 images. This is an 80% image capture rate, but once again with no positive matches being made. This is another good result with the FAR at 0%.

The third gelatine test that we done we used the middle finger to try and make a false match.

9.3.1.1.6 Test 6: Gelatine Middle Finger Verification

The same situation as the two previous tests, a Smart Card enrolled with the original fingerprint.

Attempts: 20	Image Captured: 14
No Image: 6	FAR: 0%

The third of our gelatine finger tests gave us similar results to the first two tests. The FAR was once again 0%, with a 70% image capture rate, that is 14 images captured out of a possible 20.

With the next test we wanted to see if a gelatine finger can be enrolled to the system. First we tried the gelatine thumb.

9.3.1.1.7 Test 7: Gelatine Thumb Enrolment

In this test a Smart Card was formatted and ready for enrolment. We then tried to enrol the gelatine finger to the Smart Card. 10 Enrolment attempts where made.

Attempts: 10	Failed: 10	Success: 0

From the 10 attempts, all the enrolments failed. The fingerprint scanner was only able to pick up half of the fingers presented. The other half of presented fingerprints weren't recognized as fingerprints, giving us a 50% image capture rate. The fact that four images in a row couldn't be captured for enrolment, resulted in the "failure". From a security point of view this wasn't a failure, this was a very good result.

Next we will see the test results for the enrolment of the middle finger made from gelatine.

9.3.1.1.8 Test 8: Gelatine Middle Finger Enrolment

The setup is the same as test 7. We want to enrol the middle finger to a clean card in 10 attempts.

Attempts: 10	Failed: 10	Success: 0

The results of this test proved to be the same as the results from test 7. In 10 attempts we had 10 failures. The fingerprint scanner was only able to pick up 71.43% of the fingers presented, the rest of the fingerprints weren't recognized as a fingerprint. This was yet another unsuccessful attempt to spoof the system.

The next test was the first to deliver some interesting results. In this test we tried to enrol the gelatine index finger to a Smart Card.

9.3.1.1.9 Test 9: Gelatine Index Finger Enrolment

In this test, as with the others, we use the gelatine index finger and try to enrol that to a Smart Card. 10 Enrolment attempts were made.

Attempts: 10	Failed: 9	Success: 1

This was the first time that we had any success with a gelatine finger. We got the finger enrolled to the Smart Card. This gives us a FAR of 10% for this test. The overall FAR rate for test 7, 8 and 9 using gelatine fingers for enrolment is 3.33%.

The results of test 9 prompted a new test. This test would check to see what the chances are of a person enrolling with a gelatine finger, and then being successfully authenticated using the same gelatine finger.

9.3.1.1.10 Test 10: Enrol and Verify with Gelatine Finger

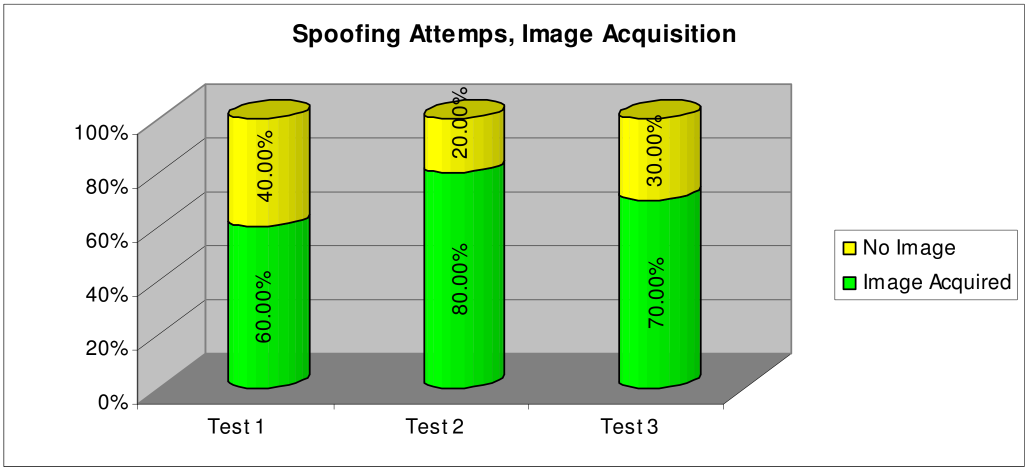
In this test, the Smart Card with the enrolled gelatine finger will be used. The same gelatine finger will be used to try and get a match.

Attempts: 20	Failed: 19	Success: 1

In 20 attempts to get a match with the gelatine finger, only one was successful. This gives us a success rate of 5%.

We have a FAR of 3.33% for test 7, 8 and 9 using gelatine fingers for enrolment, and a success rate of 5% for verifying the gelatine finger against the enrolled gelatine finger template. This means the chance that a person can enrol himself with a gummy bear (gelatine) finger and successfully authenticate himself at a later stage is 0.17%. This percentage is very low, and considering that the security settings are at their lowest, this is a good result, even better than expected.

The graph below shows the three enrolment attempts with the gelatine (gummy bear) finger. The three tests combined had an average image acquisition rate of 70%, with no successful authentications.



Next we will look at the second fingerprint match decision accuracy rate, False Rejection Rate (FRR).

9.3.1.2 False Rejection Rate (FRR)

We would like to keep the False Rejection Rate as low as possible. Valid students must be able to gain access and not be rejected. Several factors play a role here. A better quality enrolment template can produce a lower FRR. The other factor that will play a role is the consistency of the presented finger, for example finger placement.

For the following tests we did three tests in each environment just to get more accurate averages for the tests. The environment stayed the same for each of the three tests.

9.3.1.2.1 Test 1-3: Enrolled Oily Finger, Clean Finger Verification

In these 3 tests we enrolled oily fingers on 10 Smart Cards. We then used clean fingers for the verification process. The idea of these tests was to see the False Rejection Rate, and the effect that oily substances would have on the finger capture and verification process.

Test 1:	Attempts : 20	Success: 17	Failed: 3
Test 2:	Attempts : 20	Success: 19	Failed: 1
Test 3:	Attempts : 20	Success: 18	Failed: 2

In each test 20 verification attempts were made. As can be seen from the table, each test gave different results. The average FRR over the 3 tests are 10%.

In the next FRR test we will see the results when an oily finger is used for verification.

9.3.1.2.2 Test 4-6: Enrolled Oily Finger, Oily Finger Verification

For these tests we enrolled oily fingers into the Smart Cards. For the verification part of the tests we used oily fingers. The assumption would be that the FRR will be very low as the fingers are the same at enrolment and verification. This is in fact not true, the oil provides a cover over the finger and results in a lower quality image.

Test 4:	Attempts : 20	Success: 19	Failed: 1
Test 5:	Attempts : 20	Success: 17	Failed: 3
Test 6:	Attempts : 20	Success: 15	Failed: 5

Each test had 20 verification attempts. The test results got worse with every test although the environment stayed the same. The reason for this can be oily residue left on the fingerprint scanner and affecting the image quality. The average FRR for the 3 tests are 15%.

The first 2 FRR tests we used oily fingers for enrolment. The next 3 tests we will use clean fingers for the enrolment process. This will hopefully provide us with better results.

9.3.1.2.3 Test 7-9: Enrolled Clean Finger, Dirty Finger Verification

In these tests we used dirty fingers for verification against the best possible enrolment template that we can have.

Test 7:	Attempts : 20	Success: 20	Failed: 0
Test 8:	Attempts : 20	Success: 19	Failed: 1
Test 9:	Attempts : 20	Success: 20	Failed: 0

In each test we had 20 attempts, and only 1 failed. This gives us a FRR of 1.67%, the lowest yet, and a lot better than any of the previous tests.

Our next FRR test will look at the verification of oily fingers against an enrolment template of clean fingers.

9.3.1.2.4 Test 10-12: Enrolled Clean Finger, Oily Finger Verification

We enrolled clean fingers into the Smart Card. For verification we used oily fingers.

Test 10:	Attempts : 20	Success: 20	Failed: 0
Test 11:	Attempts : 20	Success: 19	Failed: 1
Test 12:	Attempts : 20	Success: 16	Failed: 4

These tests showed the same pattern as the tests in 9.3.1.2.2. The initial test has good results and a low FRR, but from there the results just got worse. Once again the oily residue that is left behind on the fingerprint scanner can be the reason for this. The average FRR for the tests is 8.33%.

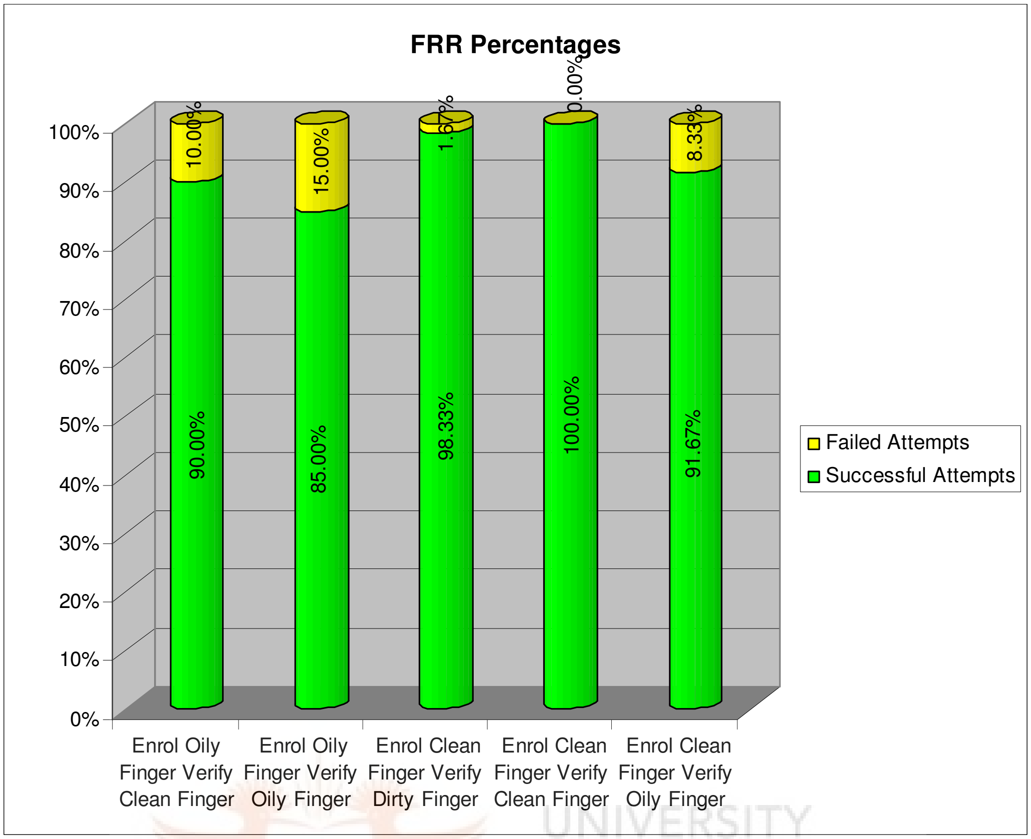
The last FRR test that we did, we used clean fingers all around. The enrolment and verification were done with clean fingers. This test will hopefully provide us with the best possible results.

9.3.1.2.5 Test 13-15: Clean Finger Enrolled and Verification

We enrolled clean fingers into 10 Smart Cards for use in this test. This test will hopefully provide us with near perfect results.

Test 13:	Attempts : 20	Success: 20	Failed: 0
Test 14:	Attempts : 20	Success: 20	Failed: 0
Test 15:	Attempts : 20	Success: 20	Failed: 0

As can be seen from the table, from the 20 attempts, every attempt was successful. No rejections. This gives us a FRR of 0%. This is the best possible result that we could have hoped for.



The graph clearly shows that using clean fingers for the enrolment and verification processes is the ideal situation. In the graph several Failure to Enrol test results are compared to each other.

Now that we have looked at all of the match decision accuracy test results we can go on to the next set of test results. In the next section we look at the enrolment failure rate.

9.3.2 Failure to Enrol Rate

These tests will show us the failure to enrol rate in different situations. First we will look at enrolment using experienced users. The users aren't new to the technology and know how it functions.

Three tests were done on the same environment to produce better averages for the tests.

9.3.2.1 Test 1-3: Experienced Users

In each test we had 20 attempts to enrol a finger into a Smart Card. At each enrolment, the finger must be presented a total of 4 times. The first 3 times are for the enrolment template, and the 4th time is used for authentication against the enrolment template. If the authentication fails, the enrolment fails.

Test 1:	Attempts : 20	Success: 18	Failed: 2
Test 2:	Attempts : 20	Success: 19	Failed: 1
Test 3:	Attempts : 20	Success: 18	Failed: 2

The test results aren't anything drastic or out of the ordinary, and are relatively constant over the 3 tests. The failure rate for these test are 8.3%.

In the next test we used inexperienced users, people using fingerprint scanners for the first time without any training.

9.3.2.2 Test 4-6: Inexperienced Users

This test used 10 Smart Cards and 20 attempts in each test. The idea is to see if inexperienced users will have a higher failure to enrol rate. Because the users are new to the technology and may not fully understand how to use it, they may struggle to enrol successfully.

Test 4:	Attempts : 20	Success: 17	Failed: 3
Test 5:	Attempts : 20	Success: 18	Failed: 2
Test 6:	Attempts : 20	Success: 18	Failed: 2

With only 7 failed attempts out of 60, we have a failure to enrol rate of 11.67%. A little lower than experienced users but still satisfying.

In the last of our failure to enrol test we use oily fingers to see the effect that it will have on enrolment.

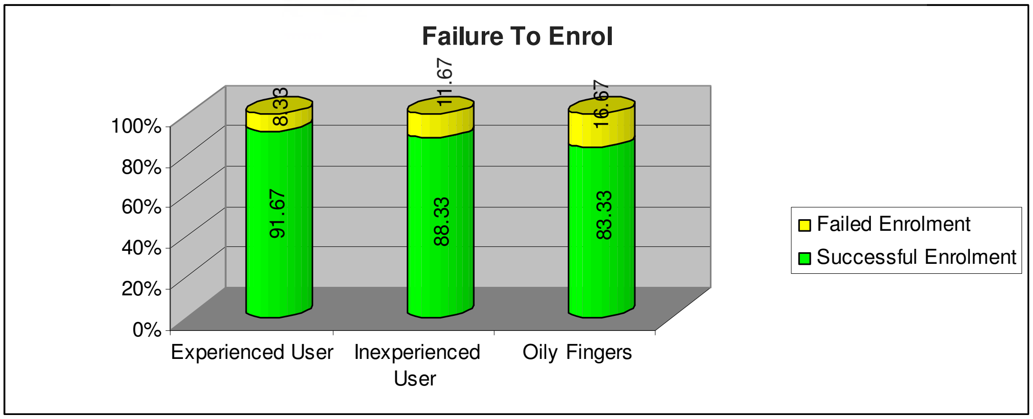
9.3.2.3 Test 7-9: Oily Finger Enrolment

We used 10 Smart Cards for this test, with 20 attempts to enrol a finger to the card in each test. All the fingers were extremely oily.

Test 7:	Attempts : 20	Success: 17	Failed: 3
Test 8:	Attempts : 20	Success: 17	Failed: 3
Test 9:	Attempts : 20	Success: 16	Failed: 4

As can be seen from the table, the results are worse than the other tests. More failed attempts were recorded. The failure to enrol rate is 16.6%.

The graph shows the results of our failure to enrol rate tests.



The next set of tests that we will look at is the failure to acquire rate. This is the rate at which the scanner is able to successfully pick up fingerprints.

9.3.3 Failure to Acquire Rate

This rate will be influenced by finger placement, movement of the finger while an image is being captured and oily residue on the finger or scanner lens. In the first test we used clean fingers.

We performed three tests on each environment to get better averages.

9.3.3.1 Test 1-3: Clean Fingers

In these tests the finger is placed on the fingerprint scanner, and we look at the message that the systems gives us. The messages can be in the line of “Too Left”, “Too Low” and “No Finger” when a finger isn’t picked up. In some cases when the scanner failed to acquire an image, it would give the message “Clean Sensor”.

Test 1:	Attempts : 40	Success: 33	Failed: 7
Test 2:	Attempts : 40	Success: 37	Failed: 3
Test 3:	Attempts : 40	Success: 37	Failed: 3

In each test we had 40 attempts where the scanner had to capture the finger. The table shows the number of failed attempts for each test. The overall failure to acquire rate for these tests are 10.83%.

The next tests will show the failure to acquire rate for oily fingers. From previous tests we can expect a higher percentage than for clean fingers.

9.3.3.2 Test 4-6: Oily Fingers

For this test we used oily fingers to access to rate at which the fingers will not be captured.

Test 4:	Attempts : 40	Success: 34	Failed: 6
Test 5:	Attempts : 40	Success: 33	Failed: 7
Test 6:	Attempts : 40	Success: 32	Failed: 8

The results for this test were worse than for clean fingers, this was expected. The average failure to acquire rate for this test is 17.5%.

The last failure to acquire test that we will look at is done with dirt on the finger tips. The idea of this test is to see if dirt will have an impact on image acquisition.

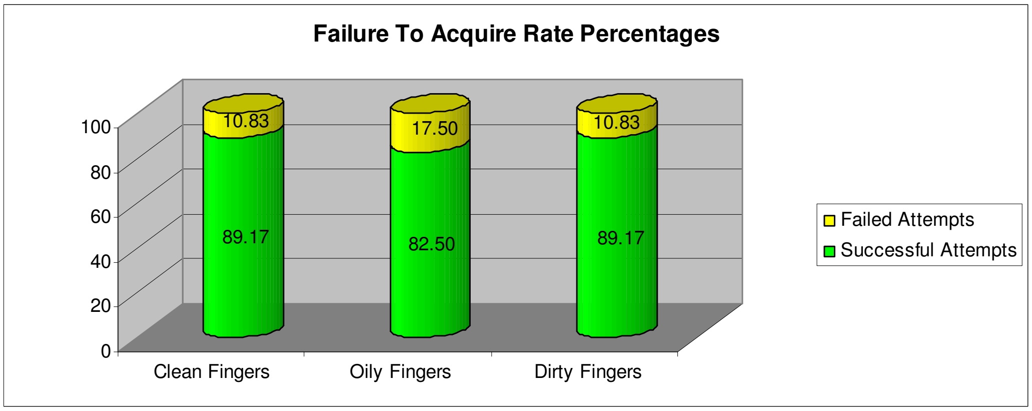
9.3.3.3 Test 7-9: Dirty Fingers

The finger tips were completely covered by dirt. The question is if the dirt would play a part in making it difficult for the scanner to pick up the image.

Test 7:	Attempts : 40	Success: 36	Failed: 4
Test 8:	Attempts : 40	Success: 34	Failed: 6
Test 9:	Attempts : 40	Success: 37	Failed: 3

As can be seen from the table, the dirt didn’t make a big difference. In fact, the dirty fingers got the same failure to acquire rate as clean fingers, 10.83%.

The graph displays the results for the Failure to Acquire Rate tests. Clean fingers and dirty fingers got the same results.



We have now looked at match decision accuracy rates, failure to enrol rate and the failure to acquire rate. Next on the list are multiple attempt error rates.

9.3.4 Multiple Attempt Error Rates

This test will show us the number of times that the first attempt was successful and the number of times that a second or third attempt was needed for verification. The Multiple Attempt Error Rate will be the rate at which a second or third attempt was needed to verify a fingerprint. These tests were done with 9 Smart Cards as one of them is malfunctioning. First we will look at the results from clean fingers.

Once again we performed three tests on the same environment to get better averages for our test results.

9.3.4.1 Test 1-3: Clean Fingers

In these tests we presented clean fingers for verification, with each test having 27 attempts. We expected very good results for this test.

Test 1:	Attempts: 27	1st Attempt: 26	2nd Attempt: 1	3rd Attempt: 0
Test 2:	Attempts: 27	1st Attempt: 26	2nd Attempt: 1	3rd Attempt: 0
Test 3:	Attempts: 27	1st Attempt: 25	2nd Attempt: 2	3rd Attempt: 0

The 1st attempt success rate for this test was 95.06%. This left us with a multiple attempt error rate of 4.94%. No 3rd attempt was needed for any of these tests.

In the next test we will look at oily fingers and their attempt rates.

9.3.4.2 Test 4-6: Oily Fingers

We had three tests with 27 attempts at verification each, which are 9 cards with 3 attempts each.

Test 4:	Attempts: 27	1st Attempt: 25	2nd Attempt: 2	3rd Attempt: 0
Test 5:	Attempts: 27	1st Attempt: 20	2nd Attempt: 5	3rd Attempt: 2
Test 6:	Attempts: 27	1st Attempt: 23	2nd Attempt: 1	3rd Attempt: 3

Oily fingers gave us a 1st attempt success rate of 83.95% which is significantly lower than the 1st attempt success rate of clean fingers. The 2nd attempt success rate is 9.88% and the 3rd attempt rate is 6.17%. This comes down to a multiple attempt error rate of 16.05%.

The last multiple attempt error rate test that we will look at is done with dirty fingers.

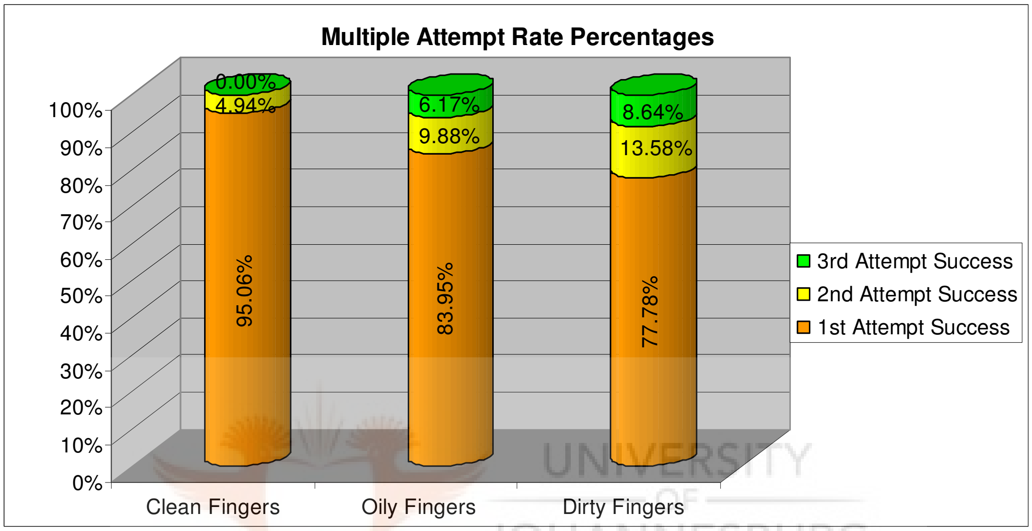
9.3.4.3 Test 7-9: Dirty Fingers

This test is the same as the 2 previous tests, 3 tests with 27 attempts each, using 9 Smart Cards.

Test 7:	Attempts: 27	1st Attempt: 22	2nd Attempt: 2	3rd Attempt: 3
Test 8:	Attempts: 27	1st Attempt: 18	2nd Attempt: 6	3rd Attempt: 3
Test 9:	Attempts: 27	1st Attempt: 23	2nd Attempt: 3	3rd Attempt: 1

These tests gave us the worst results of all the multiple attempt error rate tests. The 1st attempt success rate is 77.78%. The multiple attempt error rate is 22.22%. The 2nd attempt error rate is 13.85% and the 3rd attempt rate is 8.64%. This is the highest rates of these tests by far.

Clean fingers had the best multiple attempt rates, and surprisingly dirty fingers had the highest rate. These results are displayed in the graph.



The next test is a quite important test for any access control system. In a lot of cases the results of this test may determine whether the system will be used or not.

9.3.5 User Throughput

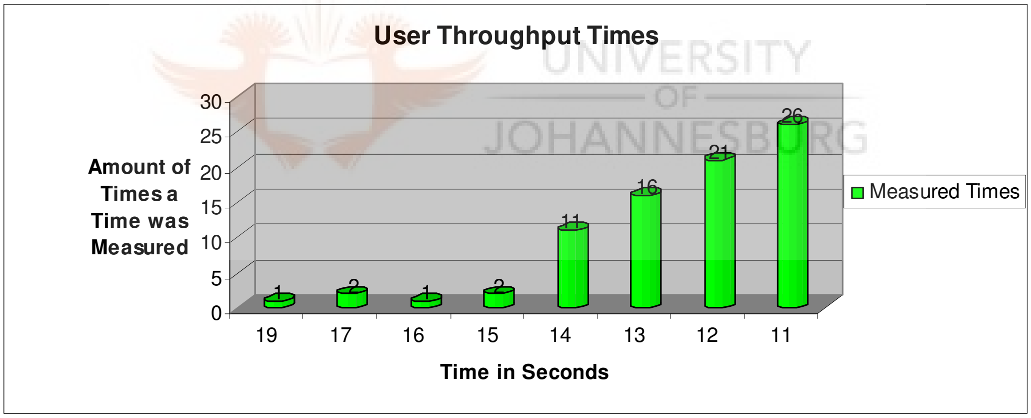
This test will show us how many people can pass through the system in a certain amount of time. This is a really important test for any access control system.

We measured the time for a group of ten people, and also each individual's time. This gave us the results displayed in the table below.

Time for 1 Authentication	
Minimum Time:	11s
Maximum Time:	19s
Average Time:	12.48s
Time for 10 Authentications	
Minimum Time:	1Min 52s
Maximum Time:	2Min 19s
Average Time:	2Min 4.8s

This means that in 10 minutes an average of 48 students can authenticate themselves.

The graph shows us the number of times a certain time was recorded. Although the average is 12.48s, 11s was recorded the most times.



9.4 Summary

We have done all the tests on the system that we wanted to do. The results are satisfying, with no real surprises. The good news is that no false matches where made at the lowest security level.

We were able to enrol a gummy bear finger at least once in 30 attempts, and then authenticate it only once in 20 attempts. This means there is a 0.17%

chance that a person can enrol and authenticate himself successfully using a gummy bear finger.

The rest of the results were as expected. The other interesting test was the user throughput. In this test it became clear that on average 48 students will be able to authenticate themselves in 10 minutes times.

The next chapter will give screen shots of the Smart Card VeriSys prototype and explain how to use the system.

Chapter 10: User Manual

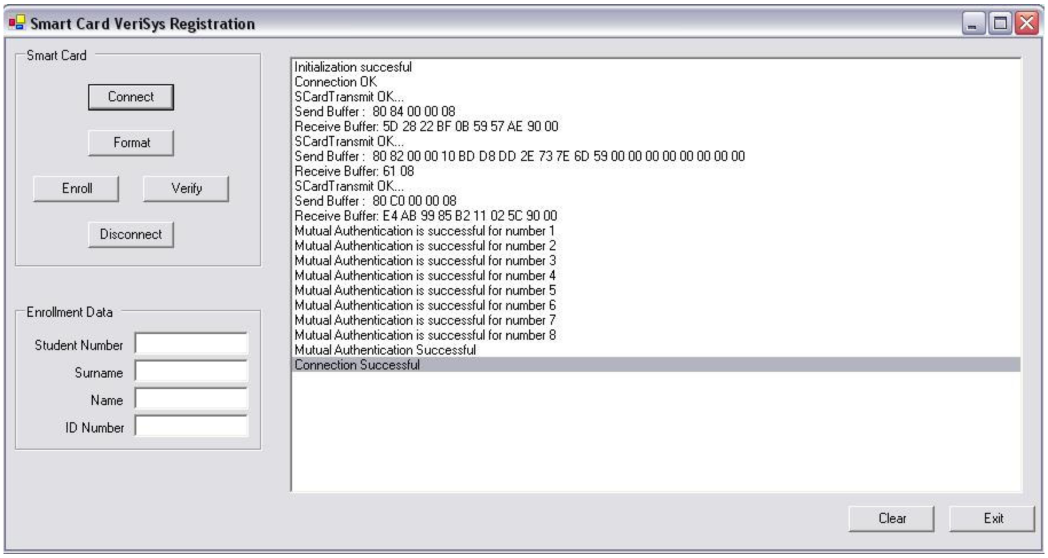
10.1 Introduction

This chapter will cover the use of the prototype Smart Card VeriSys. The program consists of two parts. The first part is the registration. This is called Smart Card VeriSys Registration. The second part is the authentication, called Smart Card VeriSys Authentication.

We will provide screenshots of the prototype and guide the user through the steps of using this program successfully. The fist part that we will look at is the registration program, as this is where every user will start.

10.2 Smart Card VeriSys Registration Manual

The first action for this part of the system is to insert the Smart Card into the reader. Once the card is in the Smart Card reader we can press the connect button. This will start the connection to the card. In the right hand box messages will be displayed, and when the connection is made, “Connection Successful” will be displayed.



```
Initialization succesful
Connection OK
SCardTransmit OK...
Send Buffer :  80 84 00 00 08
Receive Buffer: 5D 28 22 BF 0B 59 57 AE 90 00
SCardTransmit OK...
Send Buffer :  80 82 00 00 10 BD D8 DD 2E 73 7E 6D 59 00 00 00 00 00 00 00 00
Receive Buffer: 61 08
SCardTransmit OK...
Send Buffer :  80 C0 00 00 08
Receive Buffer: E4 AB 99 85 B2 11 02 5C 90 00
Mutual Authentication is successful for number 1
Mutual Authentication is successful for number 2
Mutual Authentication is successful for number 3
Mutual Authentication is successful for number 4
Mutual Authentication is successful for number 5
Mutual Authentication is successful for number 6
Mutual Authentication is successful for number 7
Mutual Authentication is successful for number 8
Mutual Authentication Successful
Connection Successful
```

Figure 10.1: Smart Card VeriSys Registration Screenshot

The next step is to format the card by pressing the “Format” button. To enrol a person we enter the user’s information into the text boxes and then press the “Enrol” button. The user will be asked for his fingerprint a total of 4 times. The first 3 times will be used for the template and the fourth is for verification of the template.

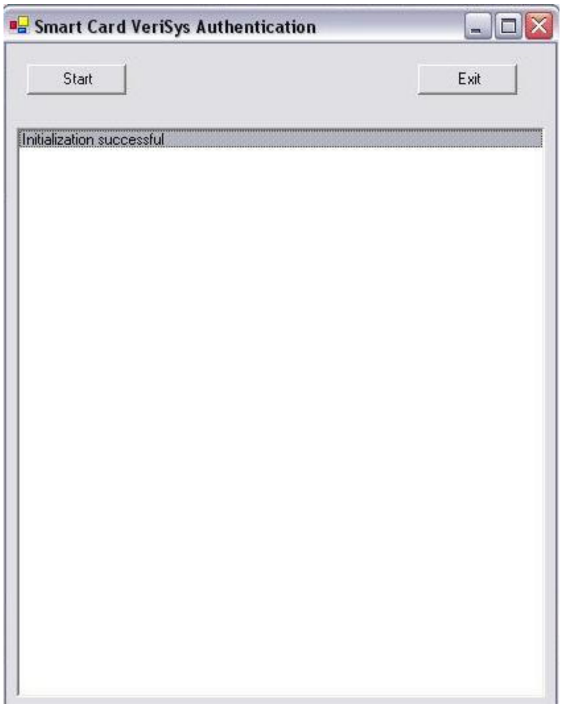
When enrolment is done we can disconnect the card by clicking on the “Disconnect” button. The card can now be removed from the card reader.

On the user interface there is an extra “Verification” button that can also be used to verify the finger against the template.

The “Clear” button clears the message area, and the “Exit” button ends the program.

10.3 Smart Card VeriSys Authentication Manual

The authentication part is really easy to use. First we press the “Start” button. Then we can insert a Smart Card into the card reader and the program will automatically pick up the Smart Card and connect to it.



Initialization successful

Figure 10.2: Smart Card VeriSys Authentication Screenshot

The program will ask the user for his fingerprint. If the fingerprint matches the template on the Smart Card then the user will be granted access. He can now remove his card from the reader. The next Smart Card can be inserted immediately and will be picked up by the program. It is not necessary to click on the "Start" button again.

To end the program we simply press the "Exit" button.

Chapter 11: Evaluation of the Results

11.1 Introduction

This chapter will take a look at our problem statement, proposed solution and objectives of the thesis. We will then discuss some of the test results to see if the solution will work and solve our problem statement.

We will now take a look at the evaluation.

11.2 Evaluation

The problem statement of this thesis from Chapter 1 states that: when using magnetic stripe cards and RFID cards there are no way to positively identify the presenter of the card as the true owner.

In that same chapter we proposed the following solution: to use Smart Cards combined with biometrics to truly identify the person presenting the student card. This way we use something the user has and something the user is to improve the security.

Our main objective from the start was to see if we can enforce better security and student identification using the Smart Card and fingerprint identification. We only want to allow access onto the campus to registered students with the correct card. A student that borrowed a card should not be allowed onto the campus.

Two tests in particular were really important for us to see if we succeeded in our objectives. The tests are: False Acceptance Rate and False Rejection Rate.

In the FAR (False Acceptance Rate) test the rate was 0% for every test conducted on the prototype. We enrolled fingers to Smart Cards and then tried to spoof the prototype by using fake or gelatine fingers. These attempts failed and resulted in a FAR of 0%.

We were however able to enrol a gummy bear finger at a success rate of 3.33%. The verification of the same gummy bear finger against the enrolled gummy bear finger template had a success rate of 5%. This means that there is a 0.17% chance that a person can enrol a gummy bear finger and successfully authenticate himself again with that finger.

The FRR (False Rejection Rate) got varying results over the 5 tests conducted. The average FRR for the 5 tests are 7%. The most important test from the five is: clean fingers were used for enrolment, producing the best possible enrolment template. Then clean fingers were used for verification, giving us a FRR of 0%. With the best possible enrolment template the FRR will always be very low if not 0%.

From these two tests we can see that this prototype system will succeed in our objective of improved security and student identification. Only registered students with their own card will gain access to the University campus and exam venues.

It is now possible to truly identify the presenter of the card as the true owner of that card. This proves that our proposed solution of combining Smart Cards and biometrics for access control will indeed provide better security and identification of the presenter of the card.

Appendix A: DES Encryption

To understand encryption better we will start by looking at encryption algorithm terminology.

A.1 Encryption Algorithm Terminology

This is just a quick reference to some of the most commonly used terms when looking at encryption algorithms (see [24]).

A.1.1 Cryptosystem or Cipher System

This is the art of changing a message so that only certain people will be able to read and understand the message. This is done with the help of an algorithm. The people that the message is intended for will also need to use the same algorithm and key to be able to read the message.

The second encryption algorithm term that we will look at is cryptography.

A.1.2 Cryptography

Cryptography is the creation of cryptosystems or the usage of these systems.

Older encryption algorithms like DES can be cracked, and that is where our next terminology comes in.

A.1.3 Cryptanalysis

When an attacker is able to break (crack) a cryptosystem and read the encrypted message.

The fourth encryption algorithm term that we will look at is cryptology.

A.1.4 Cryptology

This is the study of cryptanalysis and cryptography.

When using encryption algorithms, we transform the original message so that it is unreadable to people, this action is our next term.

A.1.5 Ciphertext

The message after encryption is called ciphertext. The message is in unreadable form.

Before we encrypt ciphertext or when we decrypted ciphertext we will get plaintext. That is our next terminology in encryption algorithms.

A.1.6 Plaintext

The message before encryption, no changes made to it.

The last two terminologies that we will look at are the terms that describe the actual use of a cryptosystem.

A.1.7 Encryption

Encryption is the name giving to the process of sending plaintext through a cryptosystem to convert it to ciphertext.

A.1.8 Decryption

Decryption is the process of changing ciphertext back to plaintext with the use of a cryptosystem.

A.2 DES

The Data Encryption Standard (DES) or also known as the Data Encryption Algorithm was developed in 1974 by a team from IBM. In 1977 this algorithm was adopted for commercial use by NIST, the National Institute for Standards and Technology (see [26]). NIST decided in 1997 that they need a new and stronger algorithm to be used as the national standard algorithm. This came after DES was cracked using brute force.

The reason why DES can be cracked by brute force is because of the small key that DES uses for encryption – only 64 bits. A longer key will have better security, for example a 192 bit key will be perfect. The strength of these encryption algorithms lie with the key that is kept secret. The algorithm is made public and can be studied by anyone and this won't weaken the security of the encryption algorithm.

A.2.1 Cryptographic Security

Security of a cryptographic system depends on a few factors (see [24]):

1. Length of the key used (64 bit or 192 bit),
2. Mathematical soundness of the algorithm,
3. Mode of operation,
4. Key management and
5. Implementation.

When a message is encrypted with DES, the receiver is able to authenticate the sender. This means that the receiver will know who the sender of the message is. The receiver will be able to check the integrity of the message. Lastly, non-repudiation will be achieved when using DES. The sender of a message cannot deny sending the message. The reason for this is that the sender and receiver share a secret key (see [24]).

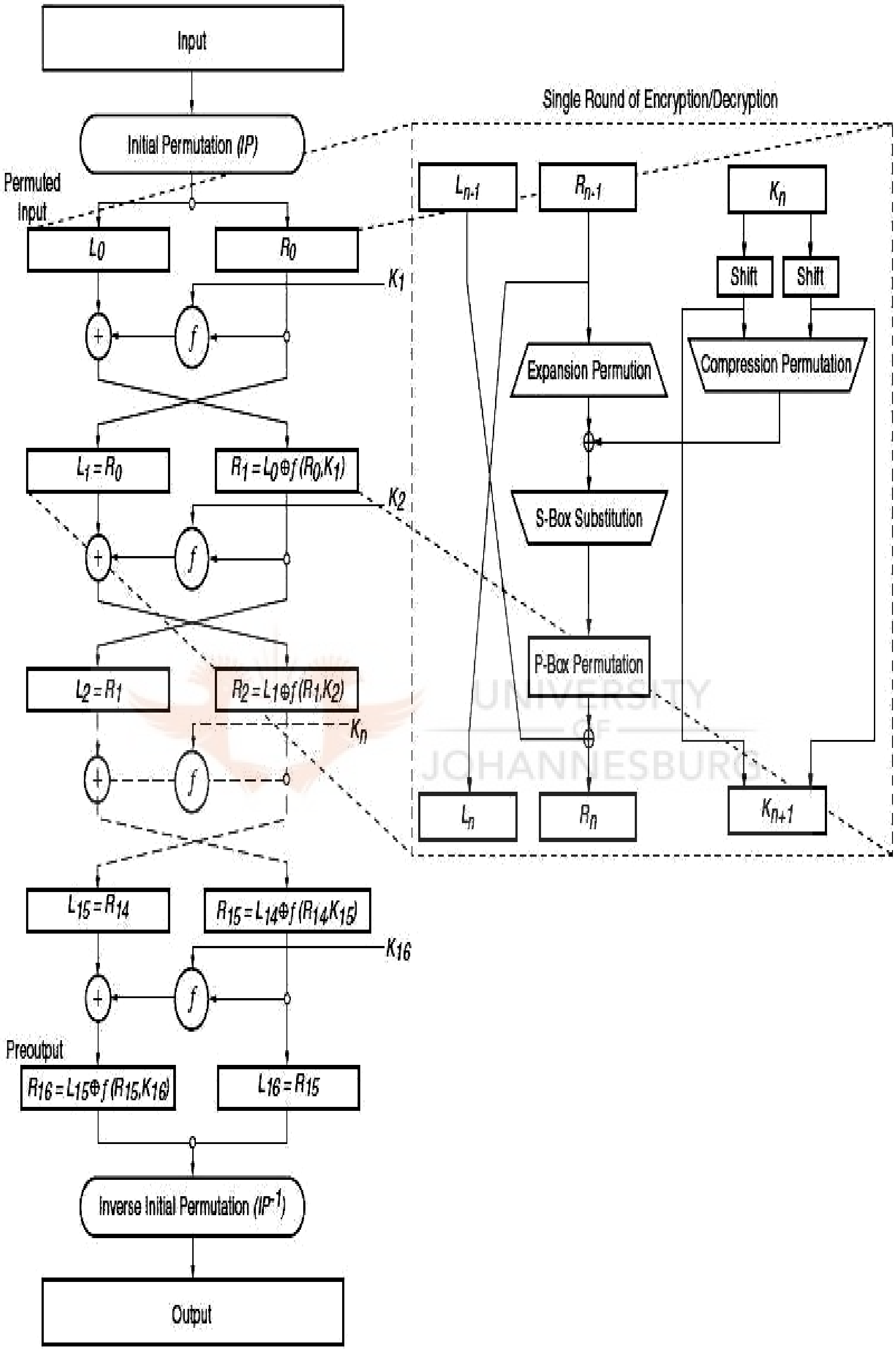


Figure A.1: DES encryption algorithm

The DES encryption algorithm starts with a 64bit input data block. This data is put through an Initial Permutation (IP). After the IP the data is split into two 32bit blocks, L(0) and R(0). R(0) will become L(1), and R(1) will become L(2) and so on. Thus L(n) = R(n-1).

R(0) goes through function f, the result is XORed with L(0) to produce R(1). Thus R(n) = L(n-1) XOR f(R(n-1)). This is done for 16 rounds. After the last round an Inverse Initial Permutation is performed on the data, this then gives us the final output, the ciphertext.

Function f is as follows: the 32bits goes into an Expansion Permutation, the 32bits are increased to 48bits by creating 8 blocks of 6bits each (see [28]).

Next the 48bits are XORed with the key, which are at this stage also 48bits. The data then goes into an S-box Permutation. In this S-box the data are converted back to 32bits. 8 S-boxes are used for 6-to-4 bit substitution mappings (see [25]). And lastly the data goes into a P-box permutation for one last rearrangement of the data.

The key length is 64bits, from which 8bits is for parity checking. The 8 parity bits are 8, 16, 24, 32, 40, 48, 56 and 64 (see [24]). The remaining 56bits are then used to create 16 (or the number of rounds that DES runs) 48bit keys. The key is then split up into two 28bit keys. Each half is then shifted a few places, these two halves then produce the next key. The two halves go through a compression permutation to for a 48bit key. This 48bit key is then XORed with the data that came from the Expansion Permutation (see [26]).

Decryption with DES works in reverse with the same algorithm, the keys are also used in reverse. With decryption the first key will be K16, and then K15 and going on till K1 (see [25]).

The data that is encrypted are sent through 16 rounds of transformation. In these rounds the data are substituted, permutated and XORed, using every bit of the data and every bit of the key.

A.2.2 Substitution

Every character in the plaintext is replaced by a substitution character, for example: A is replaced with M and B with Z.
A > M, B > Z. The text is scrambled.

A.2.3 Permutation

The data is written in a fixed size block, and then rearranged, for example: take the last line of the block and use it as the first part of the message, keep on doing this till all the lines are used.

A simple message like “meet me at home in an hour” can become “t h ao ee e h emtmn rm aoinu”. The message was written downwards in four lines, and then taken line for line from the bottom upwards.

m		a	o	i	n	u
e	m	t	m	n		r
e	e		e		h	
t		h		a	o	

Figure A.2: Permutation Table

A.2.4 XOR

Also known as “exclusive or”. Takes two bits as input and gives a result back. The result is only one bit in size.

0 XOR 0 = 0

1 XOR 1 = 0

0 XOR 1 = 1

1 XOR 0 = 1

Appendix B: Triple DES

B.1 Triple DES

In 1993 a new encryption standard was needed. DES was cracked using brute force. Several new encryption algorithms were created. The one that we will discuss is a variation of DES, Triple DES.

Triple DES is precisely what the name says: 3 times DES. The DES algorithm is used 3 times to encrypt the data. For more information on the DES Encryption Algorithm see Appendix A.

B.1.1 Strengths of Triple DES

The strengths of Triple DES are:

The data are encrypted three times,
A longer key is used (can be 128 or 192 bits).

These two factors make it impossible to crack Triple DES by using brute force and currently available processing power.

This algorithm, as with DES, is public and the key is the secret. The only drawback with Triple DES is that it is slower than DES. But for the better encryption and security that Triple DES offers over DES, it is definitely worth it.

Triple DES can also be used to authenticate the sender of the message, non-repudiation will be achieved. The sender of the message cannot deny sending the message. The receiver can check the integrity of the message.

Several variations of key usage exist in Triple DES. One, two or three keys can be used for the encryption. Most widely used method is to encrypt the data with Key1, decrypt the data with Key2 and then to encrypt the data with Key3. Other variations are (see [24]):

Encrypt, Decrypt and Encrypt the data using three keys.

Encrypt, Decrypt and Encrypt the data using two different keys (like in Fig. B.1).

Encrypt the data three times in a row using three different keys.

Encrypt the data three times in a row using two different keys.

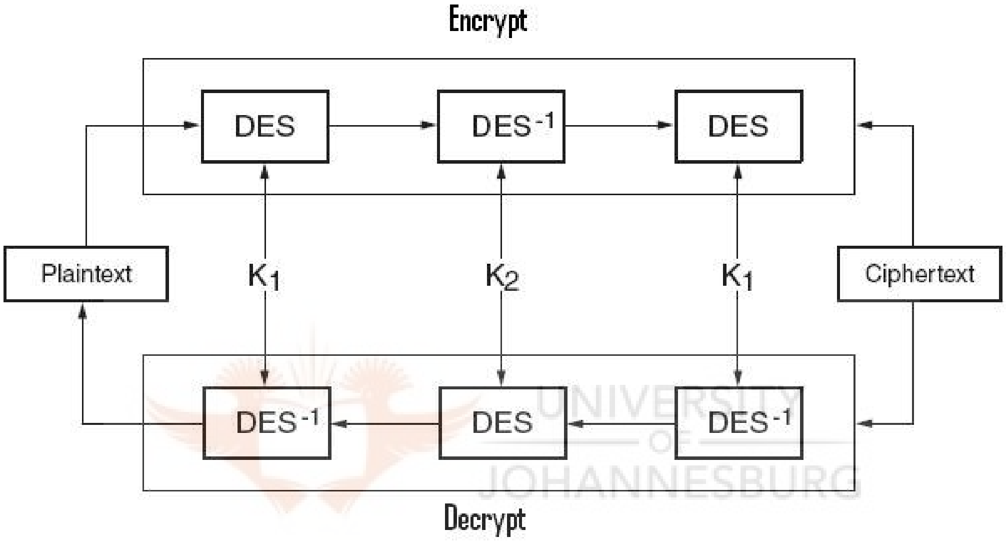


Figure B.1: Triple DES Encryption

When three keys are used, it is called a key bundle. We don’t want three identical keys in this bundle. Two options that will work for key bundles are (see [28]):

Key1 ≠ Key2, Key2 ≠ Key3, Key1 ≠ Key3, or the second option is
Key1 ≠ Key2, Key1 = Key3.

Decryption works in reverse of encryption.

Triple DES has a latency of 144 cycles, which is 48 cycles for each time DES is used (see [27]).

Appendix C: MAC

C.1 MAC

MAC stands for Message Authentication Codes and is used to check for integrity.

MAC can be used to make sure that the message really comes from who/where it says it comes from. In our program, Smart Card VeriSys, the Smart Card and the Reader will share a secret key. When the card is inserted into the reader, MAC will be used to make sure that the two parties trust each other.

C.1.1 MAC and DES

When MAC and DES are used together, the data is encrypted using DES. Then we create a value for the data using MAC. The data and the MAC value are stored together in the database. When a new MAC value is created of the encrypted data and it differs from the original MAC value, the data was changed.

MAC is also known as Integrity Check Value or Cryptographic Checksum (see [29]).

Mutual Authentication Codes are used between two parties to check the integrity of the other party.

The two parties will each compute a value from a secret key that is only shared between them, in the Smart Card VeriSys case, between the card and the reader. This value will then be compared and if it is the same the transaction can go ahead. If the value differs the transaction will be stopped.

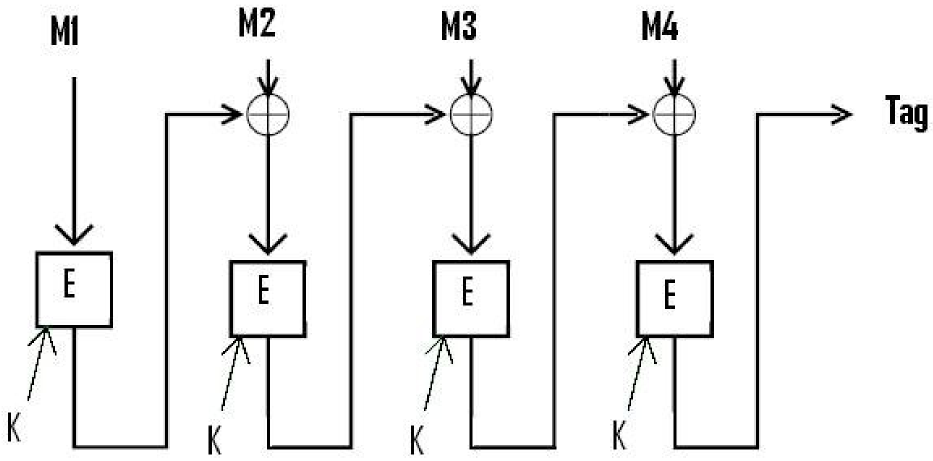


Figure C.1: MAC Tag created from encrypted message

MAC is not concerned with privacy (that is what DES is used for), MAC is concerned with authenticity.

As shown in Figure C.1, MAC needs an input message. This message will then be encrypted with a key.

References

[1] Feasibility of Smart Cards on Silicon-on-Insulator (SOI) Technology, in USENIX Workshop on Smartcard Technology, May 10-11, 1999.

[2] ACOS2 Smart Card Reference Manual, version 1.9, November 2005, Advanced Card Systems Ltd.

[3] CET Whitepaper, Steven H T Wong, China Elite Technology Co. Ltd, May 2006.

[4] Smart Cards – Present and Future, by I.Z. Berta and Z.A. Mann in Hiradastechnika, Journal on C, in December 2000.

[5] Smart Cards: Distributed Computing with $5 Devices, by C. Siegelin, L. Castillo, U. Finger in Parallel Processing Letters, Vol. 11, No. 1 (2001) 57-64.

[6] AET63 Technical Specifications, Version 1.9, 11-2005, Advanced Card Systems Ltd.

[7] Smart Card & Security Basics, by CardLogix in Smart Card Basics, DCSCB-V1.0 04/07/2000.

[8] Smart Cards: A Case Study, by J. Ferrari, R. Mackinnon, S. Poh and L. Yatawara in IBM Redbook SG24-5239-00, First Edition October 1998.

[9] Smart Cards and retailers – who stands to benefit? By S. Worthington in International Journal of Retail & Distribution Management, Volume 24, Number 9, 1996, page 27-34.

[10] Introduction to Smart Cards, by Sumit Dhar in Data Security Management 83-10-10.2, 2003.

[11] Understanding RFID technology, Chapter 2, Garfinkel book, by S. Garfinkel and H. Holtzman, page 15-36, June 2005.

[12] Position Paper: RFID and Libraries, by L.B. Ayre in Wireless Privacy: RFID, Bluetooth and 802.11, 2005.

[13] Security and Privacy in Radio-Frequency Identification Devices, by S. A. Weis, Master of Science in Computer Science at the Massachusetts Institute of Technology, May 2003.

[14] Securing e-business applications using Smart Cards, by E. M. Hamann, H. Henn, T. Schack and F. Seliger in IBM Systems Journal, Volume 40, No 3, 2001, Page 635 – 647.

[15] Improved fingerprint matching by distortion removal, by A. Senior and R. Bolle in Special Issue on Biometrics, published in IEICE Trans INF & SYST, Volume E84-D, No 7, July 2001.

[16] Introduction to Fingerprinttechnology, by G.A. Von Graevenitz, published in A&S International, Volume 53, Taipei, 2003, page 84-86

[17] ID-based password authentication scheme using Smart Cards and fingerprints, by H.S. Kim, S.W. Lee and K.Y. Yoo, in ACM SIGOPS Operating System Review Archive, Volume 37, Issue 4, October 2003, page 32-41.

[18] Precise BioMatch Fingerprint Technology, by O. Svedin, M. Öbrink and J. Bergenek, in Presice Biometrics White Paper, April 2004.

[19] Chapter 1: How Authentication Technologies Work, by R.E. Smith in Biometrics, Identity Assurance in the Information Age, 2003, page 3-23.

[20] Chapter 3: Fingerprint and Hand Geometry, by P.T. Higgins in Biometrics, Identity Assurance in the Information Age, 2003, page 45-69.

[21] Chapter 8: Biometric Liveness Testing, by V.S. Valencia and C. Horn in Biometrics, Identity Assurance in the Information Age, 2003, page 139-149.

[22] Chapter 10: Biometric Standards, by J. Stapleton in Biometrics, Identity Assurance in the Information Age, 2003, page 167-181.

[23] Chapter 2: How Biometrics Work, by J.D. Woodward Jr, N.M. Orlans and K. Raina in Biometrics, Identity Assurance in the Information Age, 2003, page 25-41.

[24] Data Encryption using DES/Triple-DES Functionality in Spartan-II FPGAs, by A. Dhir, in Xilinx WP 115 version 1.0, March 9, 2000.

[25] Chapter 7: Block Ciphers by A. Mendez, P. Van Oorschot and S. Vanstone, in Handbook of Applied Cryptography, 1996.

[26] The Data Encryption Standard (DES) and its strength against attacks, by D. Coppersmith, in IBM J. RES. Develop. Volume 38, No. 3, May 1994.

[27] High-Speed DES and Triple DES Encryptor/Decryptor, by V. Pasham and S. Trimberger in Xilinx XAPP270 Version 1, August 2001.

[28] Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, by W. C. Barker, in NIST Special Publication 800-67, Version 1, May 2004.

[29] Message Authentication using Hash functions – The HMAC Construction, by M. Bellare, R. Canetti and H. Krawczyk in RSA Laboratories' CryptoBytes, Volume 2, No1, 1996.

[30] Keying Hash Functions for Message Authentication, by M. Bellare, R. Canetti and H. Krawczyk in Advances in Cryptology – Crypto 96 Proceedings, Volume 1109, 1996.

[31] Message Authentication Codes, by J.R. Black Jr, in Doctor of Philosophy in Computer Science in the Office of Graduate Studies of the University of California Davis.

[32] International Standards Organization, www.ISO.org

[33] BioAPI homepage at http://www.bioapi.org/

[34] Smart Cards at
http://www.ewh.ieee.org/r10/bombay/news5/SmartCards.htm

[35] Introduction to Magnetic Stripe & Other Card Technologies, presented at SCAN-TECH ASIA 97, Singapore, April 24, 1997, available at http://www.hightechaid.com/tech/card/intro_ms.htm

[36] Smart Card Technology in Smart Card White Paper available at http://www.acersupport.com/library/smartcardwp.pdf

[37] Computer Algebra For Fingerprint Matching by S. Bistarelli, G. Boffi and F. Rossi, available at http://www.sci.unich.it/~bista/papers/papers-download/Paper17.pdf