UNIVERSITY OF SOUTHAMPTON

Faculty of Engineering, Science and Mathematics

School of Electronics and Computer Science

A thesis submitted in partial fulfilment for the degree of Doctor of Philosophy

Supervisor: Prof Mark Zwolinski

Smart Card Systems: Managing Risks and Modelling Security Protocols Using SystemC and Transaction Level Modelling

By

Aisha Fouad Bushager

April 2011

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

SCHOOL OF ELECTRONICS AND COMPUTER SCIENCE

A thesis submitted in partial fulfillment of the degree of Doctor of Philosophy

By Aisha Fouad Bushager

Smart cards are examples of advanced chip technology. They allow information transfer between the card holder and the system over secure networks, but they contain sensitive data related to both the card holder and the system, that has to be kept private and confidential.

The aim of the research is to conduct a risk management programme on the smart cards systems that are employed in e-business systems, suggest the best safeguards to be applied to better secure the smart card systems depending on the services and applications the smart card serves, and produce a simulation tool using a high level of abstraction programming language to be able to test the robustness of the proposed solutions.

The study contributions are producing a Risk Analysis Guide specifically on smart card systems to support managerial decision making, modelling the current and proposed smart card systems including modelling the possible attacks using the Unified Modelling Language (UML) diagrams, and developing an executable model using SystemC and Transaction Level Modelling (TLM) extensions, which is a new way of modelling and testing smart card systems security.

The security objectives have to be considered during the early stages of systems development and design; an executable model will give the designer the advantage of identifying vulnerabilities at an early stage, and therefore enhance the system security. The developed model is used to examine the effectiveness of number of authentication mechanisms with different probabilities of failure. Numbers of probable attacks on the current security protocol are modeled to identify vulnerabilities. The executable model shows that the smart card system security protocols and transactions need further improvement to withstand different types of security attacks.

Contents

Chapter 1 ..... **1**
Introduction **1**
1.1 General Background 1
1.2 Research Aim and Objectives 5
1.2.1 Research Aim 5
1.2.2 Research Objectives 5
1.3 The Importance of the Study and Contributions 6
1.4 Thesis Structure 8
Chapter 2 ..... **10**
Literature Review **10**
2.1 What is a Smart Card? 11
2.2 Smart Card Security 13
2.2.1 Identification through PINs and Passwords 14
2.2.2 Cryptographic Key Management 16
2.2.3 Public Key Infrastructure (PKI) 21
2.2.4 Biometrics 37
2.3 Smart Card Applications 56
2.3.1 Smart Cards in Payment Systems 58
2.3.2 Smart Cards in E-Government Systems (ID Cards) 60
2.3.3 Smart Cards in Health Systems 62
2.3.4 Smart Cards in Loyalty Systems 64
2.3.5 Smart Cards as Prepaid Cards in different systems 67
Chapter 3 ..... **69**
Risk Management **69**
3.1 Managing the Smart Card System Security 69
3.1.1 Asset Identification and Value 70
3.1.2 Threat Identification 71

3.1.3 Attacks on the Smart Card 72
3.1.4 Vulnerability Identification 87
3.1.5 Development of Security Requirements List 88
3.1.6 Risk Determination 93
3.1.7 Risk Mitigation 107
3.2 Concluding Remarks 109
Chapter 4 112
Smart Card System Modelling and Design 112
4.1 Modelling Languages Related Work 112
4.2 Analysing the Smart Card System using UML 114
4.2.1 Overview of the Smart Card System 115
4.2.2 The Amount of Data stored in each Smart Card Type 118
4.2.3 The Smart Card System Objects and Operations 124
4.2.4 The Smart Card System Proposed Designs 134
4.3 Attempt to Test Against Attacks by Using UMLsec 142
4.4 Concluding Remarks 143
Chapter 5 144
Smart Card System Simulation Using SystemC and Transaction Level Modelling (TLM) 144
5.1 Simulating the Smart Card System 144
5.1.1 SystemC Overview 145
5.1.2 SystemC Components 147
5.1.3 Overview of Transaction Level Modelling (TLM) 149
5.1.4 Producing the Smart Card System Simulation Tool 151
5.2 Concluding Remarks 175
Chapter 6 178
Conclusions and Future Work 178
6.1 Conclusion 178
6.2 Future Work 182
Chapter 7 185
References 185
Appendix A 199

Information Security Risk Analysis Tables 199
Appendix B 201
Publications 201

List of Figures

Figure (1): Public key Cryptography 19
Figure (2): Public Key Infrastructure Entities and Operations 25
Figure (3): Digital signatures within the PKI 27
Figure (4): Biometrics enrolment and verification processes 41
Figure (5): Smart Card Industry levels. 56
Figure (6): Identity management market expenditure forecast to 2011 58
Figure (7): Eight vulnerable points in a general Biometric System. 82
Figure (8): Bartlow and Cukic framework presenting the Biometric System Vulnerabilities. 86
Figure (9): Type of Smart Card compared to the Cost factor 98
Figure (10): Risk Matrix 105
Figure (11): Security Methods suggested to each type of Smart Card System. 108
Figure (12): Use Case Diagram- Overview of the Smart Card System 116
Figure (13): Class Diagram- The Amount of Data Stored in Each Type of Smart Card 120
Figure (14): Sequence Diagram- Using a Smart Card and a Smart Card Reader 124
Figure (15): Sequence Diagram- Biometrics Enrollment and Verification Processes in a Smart Card System 128
Figure (16): Sequence Diagram- Registration Phase in Biometrics and PKI Smart Card System. 131
Figure (17): Sequence Diagram- Verification Phase in Biometrics and PKI Smart Card System 133
Figure (18): Sequence Diagram- Registration Phase in PIN, Biometrics (Fingerprint), and PKI Smart Card 136
Figure (19): Sequence Diagram- Verification Processes in PIN, Biometrics (Fingerprint), and PKI Smart Card System. 138

Figure (20): Sequence Diagram- Verification Processes using two Biometric methods (Fingerprint and Signature), and PKI. 140
Figure (21): The Sender Module Structure of the Smart Card System 152
Figure (22): The PIN Entry Part of the Simulation Tool 154
Figure (23): Simulation Output of Transaction Flow in the Smart Card System. 155
Figure (24): Expected and Observed PIN failure attempts in PIN and Biometrics proposed model. 159
Figure (25): Expected and Observed Biometric Failure Attempts in PIN and Biometrics Proposed Model. 160
Figure (26): Smart Cards Banned in PIN and Biometrics Proposed Model. 161
Figure (27): Expected and Observed Biometrics Failure Attempts in Two Biometrics Proposed Model. 163
Figure (28): Smart Cards Banned in Two Biometrics Proposed Model. 164
Figure (29): Expected and Observed Biometrics Failure Attempts in Biometrics and PIN Proposed Model. 166
Figure (30): Expected and Observed PIN Failure Attempts in Biometrics and PIN Proposed Model. 167
Figure (31): Smart Cards Banned in Biometrics and PIN Proposed Model. 168
Figure (32): Sequence Diagram- Possible Attacks on PIN, Biometrics (Fingerprint), and PKI Smart Card System. 170
Figure (33): Simulation Output of Attack on Private Key 171
Figure (34): Simulation Output of Attack on Public Keys 173
Figure (35): Simulation output of Denial of Service Attack 174

List of Tables

Table (1): The Advantages and Disadvantages of the Security Solutions. 30
Table (2): Comparison of Biometric technologies 54
Table (3): Smart Card Information System Assets and their Values. 71
Table (4): Service phases and the related types of security requirements. 91
Table (5): Risk levels 95
Table (6): Likelihood of occurrence or probability levels 96
Table (7): Consequences levels 96
Table (8): Fraud Losses on UK-Issued Cards 2003-2008 97
Table (9): Smart Card Types Compared to Motivation Factor 100
Table (10): Smart Card Types Compared to Amount of Information Factor 101
Table (11): Factors and Elements Impact on Smart Cards 103
Table (12): Probability of attack and Consequence of attack weights 104
Table (13): Results from Testing the PIN and Biometrics Authentication Methods. 158
Table (14): Percentages of Expected and Observed PIN and Biometrics Failure Attempts. 160
Table (15): Results from Testing Two Biometrics Authentication Methods. 162
Table (16): Percentages of Expected and Observed Biometrics Failure Attempts. 163
Table (17): Results from Testing the Biometrics and PIN Authentication Methods. 165
Table (18): Percentages of Expected and Observed Biometrics and PIN Failure Attempts. 167
Table (A.1): Loss Impact Table 199
Table (A.2): Information Classification Table 200

DECLARATION OF AUTHORSHIP

I, ……,

declare that the thesis entitled

……

……

and the work presented in the thesis are both my own, and have been generated by me as the result of my own original research. I confirm that:

- this work was done wholly or mainly while in candidature for a research degree at this University;
- where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
- where I have consulted the published work of others, this is always clearly attributed;
- where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
- I have acknowledged all main sources of help;
- where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
- parts of this work have been published as:

  A. Bushager and M. Zwolinski, "Modelling Smart Card Security Protocols in SystemC TLM," in *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*, 2010, pp. 637-643.

Signed: ……

Date:……

Acknowledgements

I have devoted almost five years in pursuing and completing my doctoral requirements at one of the best universities in the United Kingdom. During this endeavour, I developed programming and simulation skills that I did not have as a business analyst, but more importantly, I realised that I am surrounded by so many wonderful people, both professionally and personally.

On a professional level, I assert my great thanks and appreciation to Professor Mark Zwolinski for his willingness to supervise me and offer the guidance I needed since the start of my MPhil/PhD program, his support and flexibility to work with my motherhood schedule made me reach the phase of submitting my final thesis. Thanks to Dr. Peter Wilson for his advices and guidance. Many thanks and appreciation to Dr.David Cabanis, Dr. Rishad Shafik, Dr. Arash Ahmadi, and Anton Kulakov for their continuous help and support on the technical and practical work.

Also, thanks to the University of Southampton for providing me with the opportunity to undertake my PhD and enrich my research skills and knowledge.I would like to express my thanks to the University of Bahrain for offering me the scholarship and funding throughout my PhD studies.

On a personal level, I would like to thank my parents and dedicate this achievement to them, without them I would not have reached this level of education. I also thank my best friend Amna AlRumaihi, my brothers and sister for encouraging me and instilling in me the confidence to achieve my goals. Most of all I would like to thank my children Mohamed and Lulwa for being able to be apart from their mom during busy working hours, and my husband for allowing me the opportunity to make my dream come true.

To my children Mohamed, Lulwa, and Shaikha...

Chapter 1

Introduction

1.1 General Background

The advances of information technology in this digital era have created new opportunities to improve the data and information transmission, implementation of new applications, and enhancement of communications over the networks. Exchanging products, services, and information, plus collaborating with other business partners via computer networks are known as electronic business [4]. More specifically, utilising information technology and electronic commerce to provide access to citizens and business partners to a range of governmental information, documents, and services is called electronic government [4].

By mentioning information transmission over networks and interactions between a government and its citizens, or a bank and its customers, concerns about information security and user privacy immediately arise. Number of questions will arise like: How does the system know that people are who they claim they are? How to pass this sensitive information through the communication channel without being intercepted or corrupted? Therefore, information system security is an essential management responsibility for e-business services generally, and e-government and e-banking services specifically.

Lately, most of the countries governments and organisations are concerned about issuing a smart card for their citizens or customers. For example, in the case of e-government, the smart card project mainly proposes a single card for citizens and expatriates that will allow access to government services such as personal identification, health, immigration, driving licence, and support an e-purse payment mechanism [5]. Therefore, this smart card is going to be used as a tool to support number of e-government applications. The main applications can be identified as following:

- E-gates: The governments are planning to implement electronic gates at the airports to support ease of transport to and from the country [5]. As such, the smart card holder will be able to benefit from quick and convenient e-gates at the airport. An additional benefit is that the smart card is considered to be a valid travel document for trips among the countries that allow such use of smart cards and e-gates because it conforms to the international standards for electronic smart cards [6], [7].
- E-health: The automation of the systems used in hospitals and medical centres lead to an efficient working environment, as it offers quick and easy access to relevant health data [8]. From this point of view, the governments decided to implement the e-health application within the e-government strategy and use the smart card as a tool to be used in governmental organisations to provide the basic medical information. Such information is going to be stored in the smart card, as well as the ability to keep track of the immunisation system that is applied by the ministry of health [9], [10]. Finally, doctors' appointments can be saved and tracked in the smart card to effectively manage the visits to the hospitals.
- E-voting: The smart card can support the e-voting technology, which is mainly practicing various election processes through the internet [5]. This way of voting will allow all eligible voters to participate in any election in

a simple and timesaving manner regardless of their geographical location. In order to identify the voter and assure a secure and confidential means of voting, the voter's details on the system are crosschecked with the biometric information stored on the card [11].

- E-purse: This application will allow the cardholder to store electronic cash within the chip at selected cash points and outlets [12], [4]. By attaching the card reader to the computer, the holder's identity is instantly and securely verified. The stored credit can then be used to pay for various services and products at the governmental facilities and selected outlets, the card holder will be able to pay government bills, fees, and benefit from automated payment systems via specially installed electronic devices at government facilities and private establishments.
- Other Online Public Services: The e-government technology will support services such as renewing driving licences, viewing birth certificates, various governmental forms, etc [5], [7]. Generally, the identification number, name, address, personal photograph, signature, and fingerprint data will be available to view at the smart card.

In addition, the e-banking system is using the smart cards instead of the normal magnetic stripe cards as a new means of payment technology in many countries [13]. These smart cards adopt the Europay, MasterCard and VISA (EMV) specification, this specification defines the technical requirements for banks that use the smart cards for Automated Teller Machines (ATM) and point-of-sale (POS) terminals [14]. The primary purposes of using a smart card are to store cardholder sensitive data securely, protect data stored on the chip against unauthorized modification, and reduce the number of fraudulent transactions resulting from counterfeit, lost, and stolen cards [13]. The smart card holds the personal details of the cardholder, account details, issue and expiry dates, and allows access to the cardholders account to obtain monetary value.

Therefore, having all these applications activated in the e-government system or the e-banking system, and accessed by number of users through a smart card raises a huge security responsibility that the management of the whole information system has to fulfil. The users will attempt to ask and enquire about the security, privacy, and risks related to this new technology that contains sensitive information like personal details and access to monetary values for each citizen in an e-government system or a customer in an e-banking system. So, it is a priority to study the security issues like availability, confidentiality, integrity, authentication, non-repudiation, and authorisation.

Governments and organisations must pay great attention on safeguarding and protecting their systems from all sorts of attacks. Also, they must be proactive rather than reactive to computer and system crimes and crises that may take place [12]. Therefore, it is vital for the management to adopt a risk management programme to be able to identify the areas that need to be audited, and to reduce the exposure faced by the governmental organisations and commercial organisations to an acceptable level of risk.

They must start by identifying their systems' assets, the value of the assets, the systems risks and vulnerabilities, recognising the possible threats and assessing the level of impact on the system components, identifying possible attacks, studying the security requirements, and finally satisfying the security requirements and goals by applying certain security safeguards. In addition, having a tool or a program that can be utilised to test the system qualities and safeguards, measure the robustness of the security measures employed, and give results of possible attacks and risks associated with the employed safeguards

will have a great impact on controlling and evaluating the system defence structure.

1.2 Research Aim and Objectives

1.2.1 Research Aim

The aim of the research is to conduct a risk management programme on the smart cards systems that are employed in e-business systems, suggest the best safeguards to be applied to better secure the smart card systems depending on the services and applications the smart card serves, and produce a simulation tool using a high level of abstraction programming language to be able to test the robustness of the proposed solutions.

1.2.2 Research Objectives

The objectives of the study are:

- To conduct risk analysis to be able to examine the threats and attacks, point out the vulnerabilities, identify risks, and determine risk levels that face the smart card system,
- To come up with possible solutions that contribute to the enhancement of the smart card system security,
- To produce models using UML, which shows the possible proposed solutions,

- To build an executable model out of the designed model by using SystemC and Transaction Level Modelling (TLM), and evaluate it in terms of system robustness and functionality.

1.3 The Importance of the Study and Contributions

It is vital to study, examine, and appreciate the latest technologies adapted and implemented by the organisations and governments in our technologically advanced era. The smart card, which is considered to be the latest trend in today's e-business environment, it is important to point out the risks behind using this type of technology, particularly when it is used on a daily basis. Thus, governments and organisations must understand the nature of the smart card transactions and exert the necessary effort to implement a successful smart card system.

In fact, successful implementation of any smart card project will support the country's communications, businesses, and government systems. It will prove how powerful and capable technology is in facilitating the day to day transactions in a secure and confident way. Risk analysis must be conducted whenever money or resources are to be spent, and exchange of sensitive data and information occurs. Therefore, being aware of the related risks of using this technology is highly recommended, and the implementation of the required security methods in a reliable, available, and usable way is extremely necessary.

The level of security of the employed smart card system in any e-business environment is the focal point of concern; hence, the study focuses on the smart card system security along with its associated risks and possible safeguards. The

first part of the study intends to conduct a risk management programme. The outcome of the programme is significant to organisations that employ smart card systems and would like to operate in an environment that can stand against internal or external risks. It allows the organisations, regardless of their areas of operation, to put into focus the smart card system security objectives, and it also serves as a guide in developing the risk analysis process that meets the organisation's business and system needs.

The second part of the study focuses on modelling and testing the proposed security mechanisms and solutions. The modelling and design process uses a well known and highly recommended modelling language like the Unified Modelling Language (UML) to produce diagrams, along with SystemC as a programming language that is of a high level of abstraction to produce a simulation tool that allows the testing of the current and proposed solutions.

The contribution of the study is to help decision makers and system analysts to take better decisions in terms of operating in safe environments, have a better idea of the possible solutions, and test their security employed schemes against possible attacks, threats, or risks. The risk analysis in this study focuses on the smart card system, which is something that has never been done before. Most risk management programmes are concerned about information technology security in general like the National Institute of Standards and Technology (NIST) risk management framework [15], but there has been no risk analysis study or guide that is conducted specifically on smart cards.

In addition, the modelling of the smart card current systems and proposed systems including the modelling of the possible attacks has not been done before,

this part of the study is successfully published in the 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, please refer to Appendix (B).

Finally, the executable model that is produced using SystemC along with its TLM extension is a new way of modelling and testing the smart card systems, and is considered as an additional contribution that supports bridging the gap between the design and implementation phases of the smart cards systems development.

1.4 Thesis Structure

The report contains six chapters. Chapter one is an introduction to the research, and it includes an explanation of the general background of the research, statement of the research aim and objectives, in addition to the importance of the study.

Chapter two provides an overview and evaluation of the related literature on the research topic; the purpose of this chapter is to help the reader develop a good understanding of the relevant previous research work and investigation that took place in similar areas of interest.

Chapter three contains the Risk Management Programme that is carried out to determine the risks associated with the usage of smart cards in e-business systems, analyses of the findings, and the discussion of the study findings.

Chapter four includes the smart card system modeling and design, and a description of the current and proposed smart card systems using UML diagrams to illustrate the transactions and operations of the system objects.

Chapter five includes an explanation and implementation of an executable SystemC model, number of tests to examine the security mechanisms employed in the system are presented in the chapter.

Chapter six revisits the arguments, theories, and results stated in the previous chapters of the research, in addition, number of concluding remarks are drawn. It also contains a section that discusses the possible future work of this study. Finally, the last chapter includes the references list.

Chapter 2

Literature Review

This Literature Review chapter provides the background required and the theories and practises related to the research field. At the beginning, an overview of the smart card is presented. The second part explains the security mechanisms that are used in the current smart card systems like the PIN and Passwords, Cryptographic Key Management, and Biometrics along with the proposed mechanisms that will enhance the security of the smart card systems. After that, a section about the smart card applications that are employed in the market today will discuss the uses of the smart card in different areas. The final section is a discussion of the review of the related literature that shows the reflection and arguments.

The developments and advances that have taken place in today's business environment especially e-commerce and related technologies such as the Java language influence the initiation and development of the smart card systems. The main determinant of the smart card product rests on the combination and the overall coherence of technologies like cards and readers manufacturing, software and hardware development, cryptographic algorithm development, customisation, etc [16]. The technology is getting more and more sophisticated; in addition, various advances and improvements take place especially in the areas of operating systems, applications, and security and cryptography. This

technological evolution played a major role in the creation and development of the smart card industry.

2.1 What is a Smart Card?

The smart card technology has been around for approximately 20 years; German inventors patented the idea of having plastic cards that contain microchips in 1968. Then the Japanese and the French have patented other versions of smart cards in the 1970s. Failures took place at first but then the technology started to bloom in the 1990s [17]. Therefore, this technology has been part of the governments' strategies and projects lately and seems to be taking place in every individual's purse. A number of reasons played a role in the massive growth of the smart card technology; those reasons are mainly related to the market. One of the reasons is the credibility of the magnetic stripe card, which has reached very low levels [18]. People are now aware of the problems and fraud that are caused by the magnetic stripe cards, so they prefer the smart cards technology. The growth of the commercial activities through the Internet had given rise to the demand of smart cards [18]. Because of the advances in technology and the evolution of the Internet, most of the people in the current era rely heavily on the Internet and have most of their daily work and business transactions done online. Thus, practicing electronic commerce requires a more consistent security card that will ensure the safe exchange of data and information online such as the smart card. In addition, [18] says that there are several applications that are growing rapidly today such as health cards, customer relationship management, and satellite television decoding, those applications are strongly linked to the smart card technology. The GSM mobile

telephony system is another developed technology that places a chip card in every user's pocket [18]. A number of well known technology companies such as IBM, Sun, and Microsoft engaged in the production and implementation of the smart card field, these efforts took place in order to cope with the demand in the market and the advances of technology.

From this point, it is important to begin with defining the smart card. The author in [17] defined the smart card as any credit card sized card with more memory than the traditional magnetic stripe card, which has an on-board embedded processor, or smart chip. Smart cards provide a cryptographic token; they are able to execute cryptographic algorithms in their embedded internal circuitry [19]; it indicates that the user's data are kept secretly and never leave the boundaries of the tamper resistant silicon chip. Tamper resistance mainly means the protection of the sensitive information stored in the chip, so tamper resistant silicon chips have features that make them capable of securing the sensitive information like the private keys. The tamper resistant chip has an active shield that once broken makes it unusable by initially destroying any data held within the chip, in addition to shutting down the operations of the chip. Hence, they are designed in a way that prevents an attacker from modifying or altering the sensitive information stored within the chips. For example, the VISA security module that is commonly used in banks to generate and check PINs has a microprocessor that performs the cryptographic operations; it contains lid switches and circuitry which interrupts power to memory when the lid is opened so that the key material stored is erased or set to zero [20], [21]. Therefore, the

features and capabilities of the tamper resistant chips employed in smart cards gives them the characteristic of being very secure.

Moreover, the technology of smart card offers the benefits of easy mobility, with the capability of storing a great capacity of information in comparison with the magnetic-based plastic cards. In addition, programs can be stored in the card that can provide rich services such as security, authentication, health record management, and alert system [22]. Thus, the smart card seems to have tremendous advantages and advances in the technology embedded in them in comparison with the old magnetic cards.

2.2 Smart Card Security

Security is a very high concern when it comes to linking number of computers or terminals together through networks. It is easy to monitor the flow of data throughout the networks by applying different techniques such as sniffing, spoofing, or session hijacking [23]. Thus, it is extremely important to secure and authenticate the traffic in the networks and systems to ensure the integrity, privacy and confidentiality of the transferred data.

Privacy and confidentiality are almost the same, they both mean that the message being transferred must be read by the sender and the intended receiver only [24]. Confidentiality implies that the information or asset is restricted to authorised users only, whereas privacy is more concerned about the identity of the individual, it refers to the ability to prevent invasions of the user's personal secrets and space, which includes any information related to identifying the personality of the user, also; it is concerned about the ability of the users to choose with whom to share their private information or asset [25].

The smart card is now known for its high level of security and is used as a tool for authentication and authorisation in today's different information systems. Still, it is imperative to go through the security techniques that are applied to the smart card to ensure security and safe information transition through the systems. The user identification is the most important security technique; there are three different methods that can be used to identify a person. The first identification method is knowledge of a secret, the second method is to test the possession of an object, and the third method is testing a specific body feature[26].

2.2.1 Identification through PINs and Passwords

This type of control is responsible of identifying and verifying the system users, processes, and information resources. One of the common practices of identification is entering a PIN, it is usually a four digit number entered using a terminal keypad or a computer keyboard and then sent to a smart card. Then the smart card compares the value that it receives with an internally stored reference value and reports the result to the terminal [27]. PINs have to be memorised by the user, therefore, the user has to choose a number that is easy to remember. The number of characters in a PIN depends not only on the desired level of security but also on the memory capacity of the average card user [27].

However, this method of security is not the best identification or authentication method because one of the simplest attacks is guessing the PIN, the probability of guessing the PIN increases if the PIN digits were less, for example, a four digit PIN has the probability 0.03% in three tries [27]. Moreover, some people have their PINs written on pieces of papers that are stored next to

their cards; others use easy numbers such as 1234 or 3333, which also increases the probability of figuring out the PIN. This indicates that this kind of method is not the best authentication method to be adapted.

The other authentication method that is widely used to secure the data through networks is Password Authentication. This method has been used for a long time because of its easiness of usage and implementation. This method generates a unique identifier (ID) and a password for every user in the network, each user has to enter his ID and password in order to have access to the network resources [28], it allows the communicating parties to verify their signatures to each other without exchanging public or private keys [28].

As stated by [29], the ID-based schemes have the following advantages: neither secret nor public keys need be exchanged, the public key directory table is not needed, and the assistance of a third party is not needed. Hence, the ID-based scheme is an alternative to public key schemes where the ID of the user is used as the public key. Furthermore, Shamir's ID-Based scheme has a fixed password; the user does not have the option of changing the corresponding key to his ID. A password generator generates a password to each user ID rather than the user himself, which means that the user cannot choose the password assigned to his/her ID after registration. In the case of compromising the user password, the user has no choice but changing the current ID to a new one with a new password. This makes the scheme less flexible and weak against the attack of replaying previously intercepted passwords [28].

Then, Yang and Shieh came up with the timestamp-based password authentication scheme, followed up by the extended version of it that is the

nonce-based password authentication scheme to be used within the smart cards [28]. These two schemes do not need the directory of passwords or verification tables to authenticate users and is based on the concepts of ID-based schemes.

However, [30] mentioned that Yang and Shieh password authentication scheme that is used in smart cards has been vulnerable to some forged login attacks [30]. Also, [31] showed that an intruder is able to construct a valid login request from an intercepted login request and then impersonate other legal users within the network by sending a forged request to the remote host [31]. This indicates that the password authentication scheme is not the best authentication method that ensures a high level of security within a system though few scientists and researchers like [32], [33] and [34] have spent effort in improving Yang and Shieh's scheme. Therefore, using other types of authentication methods is required to ensure the safe and secure transmission of information within the smart card system.

2.2.2 Cryptographic Key Management

Cryptography is the science of keeping secrets secret [35], where the mechanisms of cryptography achieve the security main objectives like confidentiality, integrity, authentication, and non-repudiation. The fundamental task of cryptography is to allow the users to communicate securely over an insecure channel in a way that guarantees their transmissions' privacy and authenticity [36]. Moreover, cryptography is the study of the methods used to encrypt and decrypt data using keys. The great idea behind using the encryption and decryption processes is to make it difficult, expensive, and time consuming for an unauthorised person to have access to confidential and private data [37].

Therefore, key generation, distribution, and storage must be securely managed. The objectives of cryptography are Confidentiality, Integrity, Authenticity, and Non-repudiation [37]. Thus, cryptography is an important technology that has to be applied to ensure secure transmission of data through the public networks especially the Internet.

Any encryption method consists of three types of data: plain text (unencrypted data), cipher text (encrypted data), and the key, which is a secret code used to encrypt and decrypt a message (one or sometimes more are required for encryption and decryption of data). These three types of data are processed by a mathematical formula used to encrypt the plain text into the cipher text and vice versa. Generally, algorithms are hard to change, for some reasons such as the easiness of making a small mistake and ending up creating a weak cryptographic algorithm, keeping the algorithm secret is difficult as well because nobody builds a cryptographic algorithm for a short period of time, so algorithms should be published and used rather than kept secret. Modern algorithms are based on Kerckhoffs' principle [38]. This principle has a clear rule, which is the security of the encryption scheme must depend only on the secrecy of the key and not on the secrecy of the algorithms. Of course this does not mean that to operate securely we could use any simple algorithms, the fact is, the more complex the encryption algorithms and keys the more secure the system would be.

There are two major encryption systems, the symmetric systems where the algorithms use one secret key for encryption and decryption and the asymmetric systems where the algorithms use different keys for encryption and decryption [39].

Symmetric Systems (Private Key Encryption)

In symmetric systems the same key is used to encrypt and decrypt the data, so the sender and receiver must share the same key without revealing it to anyone else. The problem with this scheme is the transportation of the secret key between the sender and the receiver without security exposures. Thus, this kind of security schemes can work successfully in some small organisations, however, it cannot work effectively in large organisations. For number of years the Data Encryption Standard (DES) was well-known as the standard symmetric encryption algorithm which uses a 56-bit key that ensures high encryption [39].

Basically, DES is used to encrypt and decrypt packet data; it turns clear text into ciphertext with an encryption algorithm. On the other hand, the decryption algorithm on the remote end restores the clear text from the ciphertext. It is usually used to encrypt PINS [39]. In the year 2001 the National Institute of Standards and Technology (NIST) declared that DES was being replaced by Rijndael, which is the new Advanced Encryption Standard (AES) [40]. Rijndael's standard is a block cipher standard that has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, it can be specified with key and block sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits [40]. To make it more clear, a block cipher might take a 128 bit block of plaintext as an input, and the output will be a corresponding 128 bit block of cipher text.

The transformation is controlled using a secret key [40]. Then again, the decryption algorithm takes the 128 bit block of cipher text together with the secret key and yields the original 128 bit block of plain text. Until today, AES is one of the most popular algorithms used in symmetric key cryptography.

Asymmetric Systems (Public Key Encryption)

On the other hand, public key encryption is the method that uses a pair of matched keys, a public key and a private key [41], [1]. The public key is publicly available to anyone and the private key is known only to its owner. In this method, if a person needs to send a message, then the message has to be encrypted using the receiver's public key. When the receiver gets the message, the decryption of the message is done using the receiver's associated private key [41]. Briefly, if a message is encrypted with a public key, then the associated private key is required to decrypt the message.

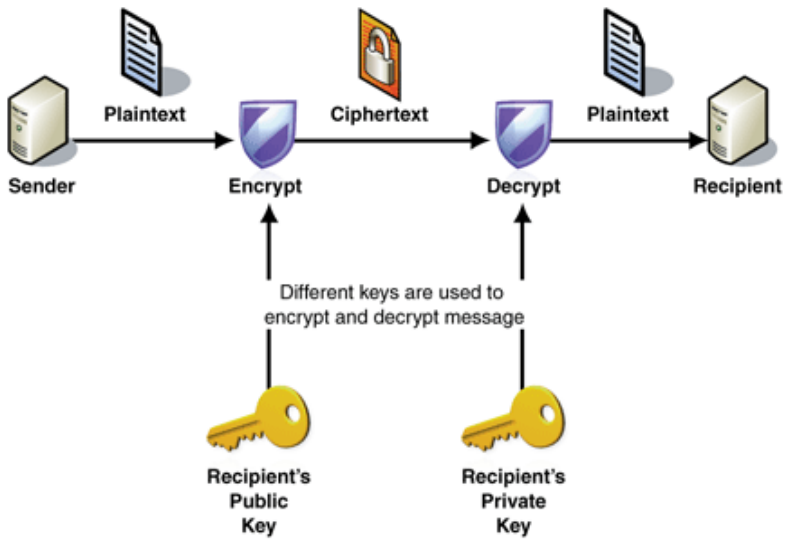

Figure (1): Public key Cryptography
Source: [1]

The best-known public key cryptography algorithm is RSA, which is named after its inventors Rivest, Shamir, and Adleman [42], [43]. It is commonly used to do public key cryptography and digital signatures based on factoring. RSA algorithm is not limited to a particular key length, it uses keys ranging in length from 512 bits to 1,024 bits; in contrast, DES is limited. This characteristic makes

the RSA better than DES for the reason that to increase security longer keys can be used without the need to modify the algorithm [41]. However, the main problem associated with this algorithm is speed [44]. Asymmetrical algorithms are generally slower than symmetrical algorithms due to the complexity of asymmetrical algorithms, so public key encryption cannot be used effectively to encrypt and decrypt large amount of data. These symmetric and asymmetric algorithms are the most well-known algorithms, therefore, they are common and used by most manufacturers.

Digital Signatures

The digital signature is the electronic version of the personal signature in the online world. It is an identifying code that is used to authenticate the sender of the message, ensure that the message contents are unchanged, and ensure non-repudiation in the future [45].

Suppose that Alice wants to send a message to Bob, at the same time Bob wants to make sure that Alice is the sender of the message and the original message contents have not been tampered with during the data transmission. The digital signature is the best solution to Bob's questions, the following is what Alice and Bob will do if the digital signature was applied to the message transmission:

Alice generates a mathematical computation known as a hash function and applies it to the message; the result of the hash function is called a message digest. Alice will also use a key generation algorithm to create her own pair of private and public keys. Then Alice is going to use her private key to encrypt the

hash, which will result in a creation of a digital signature. Finally Alice is going to encrypt both the message and the digital signature with Bob's public key and sends the digital envelope to Bob.

On the other side, Bob will then use his private key to decrypt the digital envelope and gets access to its contents (the message and the digital signature). Bob is going to use Alice's public key to decrypt the digital signature, using the same hash function employed by Alice, Bob can then creates a message digest from the decrypted message and compares the resulted message digest with the original message digest. If both messages digests match, then Bob will conclude that the message is genuine and Alice is the true sender of the message, at the same time, Alice could not deny that she is the sender of the message [46], [47].

The digital signatures are vital in achieving some of the most important security objectives like authentication, integrity, and non-repudiation [45]. However, the main problem that lies behind the usage of this technology is that Alice or the sender is not the one who computes the digital signature; it is the sender's computer that does compute the digital signature, hence, the proof that Alice is the person who signed the message is not accurate. Simply because someone else may have access to her machine and sends the message to Bob claiming that the sender is Alice, therefore, the dishonesty will take place.

2.2.3 Public Key Infrastructure (PKI)

2.2.3.1 What is PKI?

Most of the current smart card systems use the Public Key Infrastructure (PKI) technology to fulfil the system security requirements, it is until today named as the best comprehensive and secure scheme of passing information from

one point to the other. Public-key infrastructure (PKI) and digital certificates were generated to conquer the lack of presence and the anonymity of the entity that characterise insecure networks such as the Internet. PKI has number of definitions, [48] defined PKI as:

> A scheme based on public and private key cryptography and digital signatures. These signatures use software and policies that permit users to electronically encode and decode information in a secure way over the internet [48].

This definition is very brief and does not describe precisely how this security method works. The PKI contains other important elements that should be listed in the definition. The following definition is by [49] where they defined PKI in a more descriptive way:

> PKI is a security infrastructure that incorporates hardware, software, standards, and policies to create a framework for securing transmissions, verifying and validating identities and ensuring the integrity and source of data through the use of asymmetric encryption and digital certificates. PKI uses the concept of a trusted third party for implementing key life-cycle management processes [49].

This is a more clear definition of what PKI is and what the important elements in this type of security method are. A more specific definition will probably mention the digital signature and the management system of the certificates.

If the PKI is available, then digital signatures are available as well [19]. The PKI provides a framework for addressing important security considerations like authentication, confidentiality, authorisation, integrity, and non-repudiation that are extremely required to conduct business on the web [49], [48]. It mainly uses the concept of a trusted third party for implementing key life-cycle management processes. This third party is called the Certificate authority (CA),

which validates the identity of the user and issues digital certificates [50]. The following section will discuss in more details the PKI main components and their related duties.

2.2.3.2 PKI Main Components and Operations

The CA is one of the major and main PKI components that are considered to be a trusted party in managing the confidential details that are included in the digital certificates that are issued to the requesters, normally; the CA issues a policy statement indicating the company's procedures and responsibilities [48, 51]. In addition, the CA could be online where the certificates can be obtained through the network infrastructure or offline where the certificates are saved in a room and sent to the requester by using disks through a secured transport service.

For example, Verisign which is one of the well known PKI vendors in the market operates online [51]; however, some other vendors prefer to stay offline to better control the security of the stored certificates. Each CA has its way of securing the digital certificates and ensuring the safety of the certificates transport to and from the CA, it all depends on the resources available to the CA and its capabilities comparing to the requesters terms and conditions as well.

Public key cryptography uses two keys and a series of mathematical formulas to scramble and unscramble data that flow through the network as mentioned earlier [19]. PKI authenticates the users through digital certificates, the validation of those applying for a digital certificate and the verification of the associated CA are done by a Registration Authority (RA). In fact, choosing to

have a RA involved in the PKI cycle is something that is considered to be optional [50], some users just prefer to have the RA included in the system to ensure the authentication of the subscribers because the RA is a local agent that requests a certificate from the CA on behalf of the subscriber after authenticating the subscriber face to face or in other forms. Therefore, the request of issuing a digital certificate given to the CA by the RA is trusted because of the authentication of the subscriber; this is just as good as if the CA had done this authentication of the subscriber by itself. Then the CA issues the digital certificates; this is done through the use of public/private key pairs and an effective key management process.

Furthermore, there is an important process within the PKI, this process is called Revocation [43], [50]. The revocation process mainly revokes the digital certificates that are not any more valid, have been corrupted, the private key has been stolen or wrongly disclosed due to improper storage or use, the subject no longer requires the certificate, or in the case where the certificate has been stolen [43], [1]. The users are informed by the revocation process that their certificates are not any more valid to use by publishing a Certification Revocation List (CRL), which is a list signed and issued by a CA consisting of the revoked digital certificates that are not in use any more [1]. Yet, the revocation process must be done in a secure manner to prevent intruders from having the ability to revoke valid certificates. If anyone can revoke anyone else's certificates, then the system will end up being corrupted. The publication of certificates and CRLs is a very essential step that must be controlled securely to ensure the safety of the certificates.

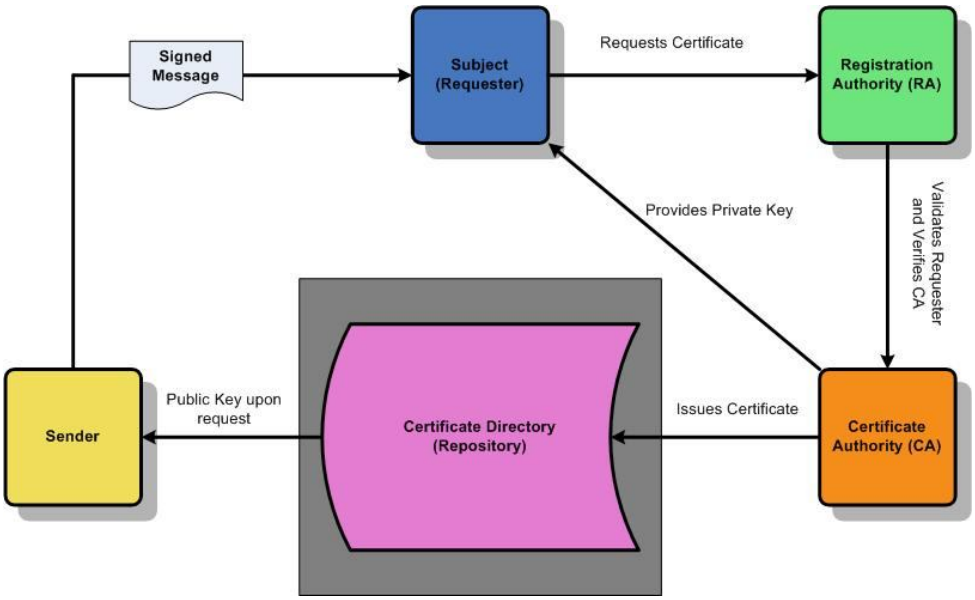

Figure (2): Public Key Infrastructure Entities and Operations

Therefore, the PKI mainly consists of a CA that issues and verifies digital certificates, a RA that authenticates the subscribers and must verify the CA before a digital certificate is issued, which is in other words the verifier of the CA, a directory or could be more than one where the digital certificates with their public keys are stored, and a certificate management system [48].

Figure (2) is an illustration of PKI's main elements and the flow of requesting and issuing a digital certificate. According to figure (2), the subject requests a digital certificate from a CA; this step has to be done by passing through a RA first for the purpose of validating the requesting party and the verification of the associated CA. Then, the CA creates a digital certificate for the requester, the most commonly used format for the certificates is X.509 [1], this certificate includes the requestor's information, an expiration date for validity, and the CA's digital signature. Furthermore, the CA creates a pair of keys (private key and public key); the private key is provided to the requesting party and the public key is stored in a repository that is publicly available to give all other parties

access to the public keys. It is imperative to mention that the private key has to be kept secret and available to the owner only, never share a private key with anyone else and never send it through a public network like the Internet.

Therefore, the sender uses the receiver's public key that is publicly available through the repository to encrypt the message, and then the message could be safely sent through any network even the Internet because the only party that can decrypt the message and have access to its contents is the receiver by using the associated private key. The PKI builds a trusted relationship between its entities that is implemented to make sure that the public keys stored in the repository are trusted. Simply because parties that are going to use the PKI technology want to make sure that the people they are communicating with are who they claim they are, and the public keys used to encrypt the data are really the keys belonging to the parties they are willing to communicate with.

Moreover, there is another issue to be pointed out, which is the digital signature part that takes place in PKI [43]. The private key is not only used to decrypt a message sent through the system, it is also used in creating a digital signature to confirm that the message has not been tampered with, in addition to, authenticating the origin of the message. To digitally sign a message, the sender passes the data through a hashing algorithm that returns a value that is unique and at the same time could not be reproduced [45]; this value is known as a one way hash. The next step is encrypting the one way hash using the sender's private key, therefore, creating the digital signature. On the other hand, the receiver decrypts the digital signature using the sender's public key that is available to the public access through the repository of public keys in the system

to get hold of the one way hash. The receiver then runs the data through the same hashing algorithm and compares the result to the one way hash that is pulled out of the digital signature of the sender to make sure the results are the same.

As a result, the receiver can prove that the message received was sent by the owner of the public key and has not been tampered with. Figure (3) shows how the message encryption and decryption in addition to the digital signature works:

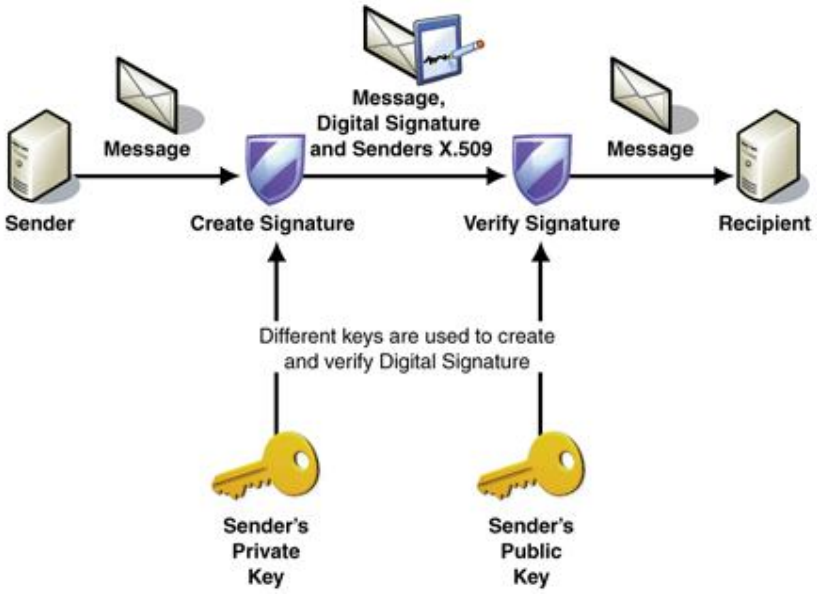

Figure (3): Digital signatures within the PKI
Source: [1]

After going through the digital signature method that authenticates the origin of the sender and ensures that the data has not been tampered with using the private key of the sender, an important question to ask here is what if the private key of the sender has been stolen? This could result in faking the sender's identity, which will result in authenticating the wrong person. In this situation, the intruder will be authenticated successfully to the system and

therefore have access to the data within the system so easily. Bearing in mind that it is possible to destroy the private key after knowing that the key has been stolen, yet, it depends on the moment the person discovers that the key has been stolen or used by someone else.

2.2.3.3 PKI Advantages and Disadvantages

Similar to any other technology, PKI has number of benefits, associated problems, and risks to be taken into consideration. It is very important to setup each system's security requirements and decide on the level security that has to be implemented to secure each type of information that flows within the system, in addition, the people that are in charge of the system security must identify the security objectives and determine which information and which person needs to be secured and how. There are number of PKI vendors that provide various versions of PKI services in the market [51], however, these services vary in price and quality. Thus, the decision on what service to chose and which vendor to select must be done in an accurate way to implement the best PKI solutions to the business.

Starting with PKI benefits, in addition to the believe that PKI is one of the best security methods available today because of its ability to secure the Internet transactions from most of the computer crimes like information or identity theft, information tampering, or other hackers problems, once the PKI software is configured the PKI solution is almost invisible to the user [48]. This indicates that this technology could be considered as user friendly because the user will only need to click on the icons that he requires and the PKI software will handle

the rest of the work, which will make the technology more easy and acceptable to the users. Another benefit of PKI is gaining the users trust by relying on a third party like the CA to manage the digital certificates and keys [43], which will perhaps ends in having the user trust the third party in handling the information privacy.

The most important benefit of establishing PKI is the ability to customise its use to fit within the application specifications, moreover, some additional toolkit approaches can be added to increase the level of customisation [49]. This indicates that the PKI appears to be one of the best security technologies that can ensure the organisations or industries different levels of security depending on each sector's requirements. PKI relies on encryption between computers; the key difference in the encryption methods applied is where the encryption control occurs. The encryption can take place in two levels, the secure network level or the secure application levels; the decision is made by the business after studying the required security level for their system [48]. Table (1) shows the possible solutions in addition to listing the advantages and disadvantages related to each solution [48].

Table (1) lists number of levels where security can take control; each method has its advantages and disadvantages. The organisations or individuals need to make clear what their needs are and indicate where the most secure levels are suppose to be implemented because each business has different products and services, therefore, has different security requirements.

Choosing to secure the network by implementing a VPN will definitely work well with organisations having number of branches or off-site employees, yet, the

difficulty takes place when it comes to performing transactions with customers or partners. Moreover, digital signatures are not provided, which means that it will be impossible to identify and authenticate the sender, only the machine can be identified to the system.

Solution	Advantage	Disadvantage
Virtual Private Network (VPN)	• Able to create a secure network over the internet • Do not need to lease lines	• Digital signatures not provided • Individuals not authenticated • Individuals do not have specific levels of trust
Secure Socket Layers (SSL)	• Compatible with popular web browsers	• Digital signatures not provided • Client authentication cumbersome
PKI Toolkits	• High flexibility	• Requires trained labour to implement and support • Implementation time • Legacy applications may not be compliant with toolkits • Requires ongoing relationship with vendor
PKI Middleware	• Client software provides SSL service • Legacy applications accommodated	

Table (1): The Advantages and Disadvantages of the Security Solutions.

The same problem exists with SSL, although the protocol has been widely accepted on the World Wide Web for authentication and encrypted communication between servers and client, no digital signatures are provided to ensure non-repudiation. Unless a proxy or a java applet is used for each connection to log on users and validate certificates there will be no possible way to avoid repudiation. On the other hand, the secure application level can be implemented using PKI Toolkits or PKI Middleware. Although the PKI toolkits

require employee ongoing training, implementation time, and a long term relationship with the vendor, it is yet a very flexible way of application security.

There are number of vendors in the market with different products and services, so organisations or individuals can agree with the vendor on the required security level and the choice of encryption software because simply these toolkits can be customised. The final solution listed in table (1) was PKI Middleware, where the software is used between the network and applications to meet the security objectives required by an organisation. Vendors provide this solution and claim it is good priced and have number of advantages comparing to other security solutions.

As a result, every security solution has its advantages and disadvantages. The decision of the solution to be implemented depends on the requirements of each system, some systems require the implementation of one of these solutions and other systems require a combination of these solutions to better achieve the security objectives of their businesses.

On the other hand, PKI like other technologies has some problems and risks associated with it. One of the problems is the consumers fear that governments might use the PKI technology as a way to invade their private and confidential information and transactions. Because of Escrow recovery the consumers do not have full trust in the PKI technology [52]. Escrow recovery is a function similar to the backup recovery of any system, however, the difference is in backup recovery the user requests the recovery of the private key or encrypted data, but in the Escrow recovery the third party can allow recovery of the user's private key to an external entity related to the government or law agencies like for

example the police in order for them to retrieve private information about the consumer without him/her knowing or authorising. Therefore, some consumers do not trust governments with access to this kind of confidential information, and conflicts between consumers and governments may arise every day and another regarding the privacy of their information and the governments' willingness to monitor transactions for discovering criminal activities.

Another important complexity that is associated with PKI implementation is interoperability. Cross-enterprise transactions are critical when it comes to organisations that rely on PKI as a security method, the reason behind this is every company, region, or even country has different standards and regulations. However, a study conducted by [38] has come up with a possible middleware mechanism that allows interoperability of PKI among different parties.

According to [38], interoperability refers to interactions of PKI operations among components in PKI application systems, each interaction might happen in different level like interactions between PKI components, different PKIs, different PKI applications, or PKI application and the PKI. As a result, PKI interoperability is considered to be multi-dimensional, which may cause problems in different levels. Therefore, the suggested middleware mechanism by [38] provides the following: hides the implementation complexity of PKI components from applications, addresses the implementation diversity of PKIs from different trust domains and different industrial sectors, and finally implements a simple system interface to application developers that meets the security and communications needs of e-commerce applications. The solution provided by [38] appears to have brought an end to the interoperability

complexity and has enhanced the interoperability of PKI; yet, the awareness of this possible way of making PKI interoperable has to be wide spread among the PKI vendors and users to better defeat the interoperability complexities that are associated with the PKI implementation and cross-enterprise activities.

The cost of relying on PKI as a security method is one of the problems that PKI users face [53], [51]. Generally, any low priced technology will most probably not include a full package of service like future upgrades or maintenance. It is the same with PKI, according to what the business requires the price of PKI will differ; if more options are required then the price of the product will be higher.

There are number of vendors in the market, so businesses have the opportunity to go and search for the best offer by the best provider of PKI bearing in mind that logically the more experienced the vendor is the better the quality of the product is. Even if the price was relatively high, the PKI technology until today is better in terms of authentication than other methods, which at the end of the day worth what the business is going to pay for.

Moreover, the CA employed in the PKI must be trusted by everybody; actually, there is no entity in the world that is trusted by all countries or every single individual. There are some different PKI models that have a single CA, a single CA plus RAs, an oligarchy of CAs, configured plus delegated CAs, anarchy, top-down, up-cross-down, and flexible bottom-up [54]. The writer in [54] has discussed the PKI models in details and stated how each model is constructed, how the CAs are organised in each model, and what the advantages and disadvantages of each model are. Then [54] concluded that the best model comparing to the other models is the flexible bottom-up where the advantages of

the previous models are within the flexible bottom-up and it allows more flexible trust rules to the CAs than the strict up-cross-down model. Hence, the decision of which model to pick is not that easy, a single CA will be risky if that CA was attacked, issued a false certificate, or went bankrupt. In contrast, multiple CA models will increase the size of the certificates because more details must be stated within the certificates, moreover, every extra CA will provide an extra point of attack, which will reduce the overall system security.

In addition to the problems, PKI has number of risks that could not be eliminated but some of them can at least be reduced to some extent. There are ten risks stated by [55], the risks are as follows:

- Who do we trust, and for what?
- Who is using my key?
- How secure is the verifying computer?
- Which John Robinson is he?
- Is the CA an authority?
- Is the user part of the security design?
- Was it one CA or a CA plus a Registration Authority?
- How did the CA identify the certificate holder?
- How secure are the certificate practices?
- Why are we using the CA process, anyway?

Taking into account the risks stated above, the PKI technology looks really unsafe to be applied to e-commerce systems. Dealing with the previously listed risks is a huge management responsibility, the people managing the PKI technology must pay great attention to the risks associated to the usage of this technology and spend enough effort in managing and mitigating the risks, in

addition to, ensuring high levels of system recovery and backup in case one or more of these risks take place.

2.2.3.4 Using Smart Cards with PKI

When it comes to the phase of storing the digital certificates and the need of having physical access to a system, the smart card technology will most probably take place. The matter of storing and transporting the user certificates in addition to the server certificates is complicated and the decision by where the certificates are to be stored is critical. According to [50]:

> Users and servers both need certificates. Server certificates are best stored in Hard Security Modules (HSMs), but more often they are simply stored on the server hard drive. User certificates, however, are probably best kept off of the computer hard drive [50].

This implies that the server certificates will anyhow be stored in the server; however, the user certificates are most likely better stored on an external token like a smart card for example. Although the smart cards are one of the best ways of keeping the certificates safe, there are some weaknesses associated with this way of storing the certificates.

One of the weaknesses is the smart cards standards [50], smart cards might not be able to talk to each other simply because there are few standards related to the smart card technology. Hence, different vendors and middleware might not have products that are able to work together, which will affect interoperability in a negative way.

Another probable drawback of storing the certificates in a smart card is the fact that the user may possibly lose the card; in this case, the user must go through the identification process with the assigned CA, where the CA will

generate a new public key value with its related information and store it in the new certificate, then the user has to validate the new certificate. So losing the card will make the user go through the identification and validation processes all over again.

At the end of the day, every technology has its strengths and weaknesses; the smart card technology has proved to be one of the well secured technologies with high level of operability. If the smart card was well managed and well secured it could be the safest way to store the certificates and private keys of the users.

Consequently, smart cards that are enabled with the PKI technology are able to protect the user's information by making them accessible to the rightful owner only. Although hackers and thieves can attack any computer system or steal any smart card, the security that is enabled within the smart card technology is hard to beat. Also, it is important to mention that the smart cards operate within number of protocols that support the PKI technology like DES and RSA [41], it depends on the protocol chosen by the system but the smart cards can work on symmetric and asymmetric protocols.

In fact, the PKI technology services have the ability to fulfil most of the security requirements in any smart card information system, yet, some requirements like untraceability and anonymity especially in the context of e-voting cannot be fulfilled. This is because PKI has a strong confidentiality, authentication, integrity, and non-repudiation features. The key management process where the users are identified physically to the CA during the registration phase, and then exchange their public keys through a public network with their identities related to it, in addition to signing the messages

via digital signatures does overcome the anonymity and untraceability features, which are required by some applications like e-voting. However, some modifications to the PKI protocols have been made recently to satisfy the highly specialised, applications specific, security requirements like anonymity and untraceability, for more details please refer to [25] and [56].

As a result, the smart card is capable of handling number of mechanisms that support the PKI technology with high level of functionality and thus ensures high level of security.

2.2.4 Biometrics

Biometrics is one of the powerful security methods among the major emerging technologies and security methods in the current digital era, it is known as one of the best identification methods used to accurately authenticate a user.

Apparently, people face various cases where they must identify and verify their personal identity to number of systems to gain access to the system components or facilities. This process is critical, failure to successfully identify and verify a user will result in harmful consequences. The previously mentioned security methods like PKI can only verify the user's computer but cannot assure the user's identity. However, Biometrics is the required method to identify and verify the transaction maker along with the password or token, which are the generally well known methods of authentication.

2.2.4.1 What is Biometrics?

The Biometrics method is based on the fact that a person possesses certain characteristics that are biologically or behaviourally unique to an individual,

which are used to confirm a user's claimed identity rather than a forgettable code or password [57], [58]. Biometrics terminology was defined by [59] as "the automated use of physical or behavioural characteristics to determine or verify the identity of an individual" [59]. Also, Biometrics can be defined as "the science of recognising a person on the basis of behavioural and physical characteristics.

Biometrics relies on who you are by one of any number of unique characteristics that you cannot lose or forget"[60]. Therefore, Biometrics is something you are, it is a powerful security method that identifies and authenticates the user without requiring the user to carry evidence like a passport or to remember the password or PIN. However, this does not mean that users can walk around without other evidence as a backup in case the Biometrics system fails.

For a biometric evidence to be ideal it has to have number of characteristics that fulfil number of requirements [61], [62], [57], the main requirements are the following:

- **Universality**: the biometric element has to exist in all people. In this respect, not all biometric elements are equivalent and the rate of distinguishing one person from another is very different, according to the type of biometrics used.
- **Distinctiveness**: the biometric element must be distinctive to each person, for example, no two persons should share the biometric. Fingerprints have a high diversification, even fingerprints of identical twins are different; moreover, the probability of two persons having the same iris is estimated as negligible. The most distinctive elements seem to be DNA, iris, retina and fingerprint.
- **Permanence**: the property of the biometric element has to remain invariant and not alterable over time for each person. While some biometrics such as iris remains stable over decades, other biometrics like a person's face or

signature's dynamics change over time. Besides, fingers are frequently injured or cracked.

- **Collectibility**: the biometric characteristic should be quantitatively measurable and readily presentable to a sensor, on other words, easy to collect. Retina scan and DNA analysis are quite intrusive, as opposed to face related characteristics and fingerprints, which are easy to obtain.
- **Performance**: accuracy, speed, robustness, and resource requirements for successful recognition should be satisfied, in order for a biometrics system to be practical and efficient.
- **Acceptability**: it is the extent to which a system is harmless and accepted by the intended users, and their willingness to use it on a daily basis without feeling annoyed or invaded.
- **Circumvention**: refers to the robustness of a system against various fraudulent methods and attacks, the ability of fraudulent methods to fool the system must be negligible.

2.2.4.2 Biometric System Components and Process

Biometric systems convert data derived from physical or behavioural human characteristics into templates, then compare the live templates with the stored templates, after the matching process produces the results, the biometric system takes decisions. Usually, every biometric system includes three major components [26]:

- A mechanism to detect, scan, or capture the image of a living person's biometric characteristic.
- Software for storing, processing, analysing, and comparing the live image with the stored image or template.
- An interface with the applications system that will use the result of matching to confirm the person's identity.

In a biometric system process, there are different stages involved:

Enrolment: is the process where the user submits the biometric sample or samples to the system via different means according to the type of the biometric sample. The method works by capturing a live biometric image of the user at the point of interaction with the system, then the image is processed using biometrical algorithms to extract the features from the image and produce a template. Finally, the template is stored in a central database or in an external token like a smart card [26]. The enrolment process takes place in both one-to-many and many-to-many systems [59], cases where users face problems with biometric systems, they need to re-enrol to be able to submit other biometric samples.

Verification: The biometrics method is used in two types of recognition, which are either identification or verification [63], [57]. Identification is a one-to-many comparison; it verifies if a person exists within a known population, therefore, the biometric sample presented by the person is compared to with existing samples in a central database [64]. The identification process confirms that the person providing the biometric sample is not enrolled with another identity and is not on a predetermined list of prohibited persons [26].

The verification process is a one-to-one comparison; it confirms that the submitted biometric evidence belongs to the person submitting it [26]. The user provides a live biometric image captured using a scanner or a reader, and then a live biometric template is created using special algorithms. After that, the live template is compared with the previously captured and stored biometric template in the smart card or the database, which was extracted during the user enrolment to the system. By using a special algorithm, a matching process

between the two templates takes place to ensure the verification or authentication of the user. The result of the matching process determines whether the person providing the biometric sample is who he/she claims to be or not.

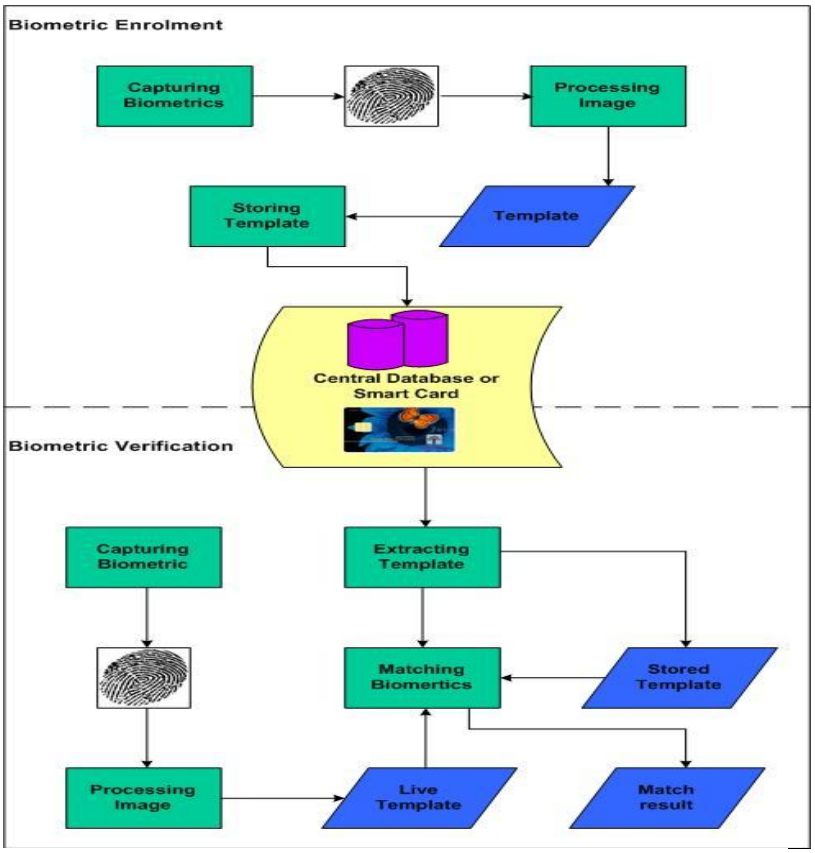

Figure (4): Biometrics enrolment and verification processes

The system performance in terms of identification accuracy can be evaluated using the false acceptance rate (FAR) and the false rejection rate (FRR) [65], [3], [57]. FAR records the situations where an impostor is accepted, on the other hand, FRR records the situations where a user or a correct person is incorrectly rejected. The system designers set this numeric score to put up with the desired accuracy level in the system, they have to tune the system sensitivity to FAR and FRR to be able to meet the system security requirements.

Furthermore, a biometric smart card is “a processor-based device which can be used to authenticate a user with a server via biometrics, there are several variants of such cards which can store the template only, perform feature extraction, or perform matching only” [58]. This indicates that the organisation has the ability to choose the kind of smart card that is equipped with the biometrics according to its needs.

As mentioned in the previous section, there are some important biometrics features that should be pointed out in order for the users to be aware when using the biometrics scheme, the features are the following: universality, uniqueness, reliability, collectability, performance, acceptability, forge resistance, and permanence [63]. In addition, not all biological features are suitable for personal identification [27]; the feature must satisfy the following criteria before it can be practically employed:

- Measured effectively
- Capable of being uniquely associated with a particular individual
- Widely distributed within the population
- Not possible to alter the feature with fraudulent intent
- Amount of reference data generated must be small
- Correct measurement of the feature must always be possible
- Both the measurement method and the feature must be acceptable to users

This points out that unless the feature satisfies the previous criteria, it is not considered to be an acceptable biometric feature to be applied to the smart card system. From this point, it is very important to take into account all the requirements of the biometrics method before and after implementing the method, this is quite critical in order to be able to make sure that the biometrics

method is going to achieve successful results once employed in the smart card system or any other information system that requires high level of security.

A study conducted by [66] proposed two signature systems that rely on biometrics, PKI, and smart cards. In one signature system, the cryptographic key is stored in the smart card and is only accessible when the signer's extracted fingerprint features match the signer's stored template. Certainly, this system is able to prevent illegal access to the private keys that are stored in the smart card, however, [66] stated that the fingerprint matching process is time consuming, and storing a template requires considerable storage space, which shows two disadvantages that stand against the successful implementation of this system.

In the other signature system, the keys are generated by combining the signer's fingerprint features, check bits, and a memorable key as named by [66]. This system has no matching process and no keys stored on the smart card. Moreover, there is generally more than one public key in this system; some pseudo public keys except a real one exist in the system. Therefore, this system does not require great storage space. Yet, this system still requires the development of some algorithms to be able to process all the required functions. So, both systems have advantages and disadvantages but trying to overcome the disadvantages of the systems may end up creating one of the best ways of combining the biometrics, PKI, and smart cards schemes in one system, in addition to providing a solution to better secure the private key.

2.2.4.3 Classification and Types of Biometrics

Biometrics can be split into two main categories physiological and behavioural biometrics, it identifies an individual by how one is or what one does.

Physiological Biometrics:

This category is based on direct measurements and data derivation of a part of the human body [59]. The physical characteristic is considered relatively stable, usually it is unchangeable and at the same time unalterable. Examples are fingerprint, facial recognition, retinal scans, iris pattern, DNA, or hand geometry.

Behavioural Biometrics:

In turn, this category is based on measurements and data derived from an action, and indirectly measure characteristics of the human body [59]. The behavioural characteristic is more a reflection on an individual's physiological makeup. Such common examples are signature, voice recognition, gate, keystroke dynamics.

Fingerprint:

The use of a fingerprint as a biometric evidence is one of the oldest techniques, best-known biometric identification method based on a physical feature, and the most widely spread biometric method, since it presents relatively few problems in terms of user acceptance and technical difficulty despite the common criminal stigma [57], [3]. In addition, it has been estimated that it is very hard to find two persons with the same fingerprint, probabilistically it is one in a billion [57], moreover, fingerprints are so distinct

that even fingerprints of identical twins are different and so is the fingerprints of each finger of each hand in the same person [62].

Fingerprints are graphical flow like ridges and valleys that take place on humans finger tips [65], most fingerprint recognition systems follow the minutiae based approach [64], other non-minutiae based approaches are directly based on the gray-scale images. The minutiae are the bifurcations and endings of the ridge lines, the feature extractor finds those bifurcations and endings from the input fingerprint images [65], [64]. Number of algorithms can be used to extract the minutiae, however, the performance of currently available algorithms relies on the quality of input fingerprint images, where fingerprint images may not always have well defined ridge structures [65].

The current electronic fingerprint sensors require the user to place the fingertip on a transparent plate, where a camera is placed under the plate to be able to scan the skin surface of the fingertip without any contact [27]. Alternatively, there are number of live scan imaging sensors that can be used to capture the fingerprints like ultrasonic sensors or semiconductor-based capacitive sensors [27], [65].

Fingerprint verification can be a good choice for many businesses or projects [3], they are expected to lead the biometric applications, the reasons behind that are simply because fingerprints are relatively low in cost, easy to integrate the fingerprint devices with the operating system in any business, and explaining to the users at the same time training the employees is an easy step that does not require lots of effort.

Retinal Pattern:

The human retina is an area at the back of the eyeball, which has a pattern of blood vessels, the pattern is formed by veins beneath the retinal surface situated at the back of the eye [67], this pattern is unique, and therefore is considered to be an accurate and feasible characteristic for recognition [3]. This technology involves analysing the retina pattern, to capture the pattern, a retina scanner is used, it is a specialised device that scans the eye from a close range [62]. The technique involves projecting a low intensity light source through the pupil, the light reflected by the retina is then collected by a camera, the recorded image data is then sent to a computer for analysis [27]. To be able to get hold of a fixed portion of the retinal vasculature needed for identification, the users must place their eyes very close to the scanner and focus on a predetermined spot in the visual filed in order to be identified [62].

Therefore, retinal scanning is one of the most accurate biometric methods, since it has the ability to uniquely identify a person with a very high degree of probability, thus, number of retinal scanning systems have been installed in several highly secure environments such as military places and prisons.

However, the cooperation of users in retinal scanning has a low degree of acceptance, since they must place their eyes very close to the scanner, which may raise the subject of anxiety, discomfort, and fear of infection [57], [67]. In addition, the retinal scanners are considered to be expensive [62], which is another disadvantage of this biometrics method. Therefore, although the technology works very well, it has not been widely accepted by users.

Iris:

People are sometimes confused with retinal scanning and iris scanning. The iris is a variable diaphragm that is responsible of controlling the amount of light reaching the retina in the eye [27], the iris is known as "the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side" [62]. It is basically the coloured ring of tissue that surrounds the pupil, which comes in different colours and styles. It is similar to the retina because it is a biological feature that is unique to each individual, which offers a very high capability of distinguishing individuals. According to [57], the probability that two irises would be identical by random chance is approximately 10^{-35}. Even the individual's left and right eyes have different iris features [57], which certainly assures that the iris is a unique biological feature that has a great ability to differentiate individuals.

In comparison with the retinal scan, the iris scan can be performed at a greater distance than the retinal scan because the process is simpler, retinal scan uses lasers that focus on the back of the eye, while iris scan zooms on the front. Iris scan makes the scanning less intrusive, as a result, the individual feels more comfortable.

An iris scanner is equipped with a digital camera that takes the picture of the eye where an infrared light is illuminated to be able to take the picture [67]. The data analysis and evaluation is very much similar to the retina scan, moreover, the iris is more readily imaged than retina; it is very hard to tamper iris texture details at the same time it is easy to detect artificial irises [62]. Eye scanning is one of the reliable biometric methods; also, it is probably the fastest growing

area of biometric research because of its promise for high scan accuracy. Yet, iris based identification and authentication systems are expensive to implement and require significant user acceptance and participation. The hardware is several times more expensive than face, finger, or palm recognition systems. Although iris or retina scanners are the most expensive biometric technologies, they are the most difficult to fool.

Hand geometry:

Is a biometric identification technique that is based on the measurements of the hand or part of the hand, these measurements can be based on number of features such as the shape of the hand, the finger spacing, the finger length and width, or the finger diameter and fingertip radius [62], [3]. This biometric technique is relatively easy to use; the user only has to place the hand on the scanner, which then performs the measurements. In addition, the hand geometry templates generated from the scan are comparatively small about 9 bytes, which requires low storage area [68], therefore, restricting their application to simple authentication purposes only.

Regarding the accuracy of hand geometry, it can be very high if desired. This method can be easily integrated with other systems and processes, so, organizations are using this biometric technique in various scenarios [3]. For example, using hand geometry in applications like time and attendance recording for employees appears to be popular.

Facial Recognition:

People are without doubt used to being recognised by their faces, that is how people are being recognised since ages, almost every ID card has the person's

photo attached to it, moreover, face recognition does not require great human interaction, so it is one of the biometric methods that are considered to be natural and easily accepted by individuals.

According to [57], face recognition can be employed using still images, multiple still images, or video sequence. The system normally uses a standard digital camera to take a picture of the face, which is a still image, or may use a digital video camera to capture a sequence of images from different angles [67], [60]. Usually, face recognition systems rely on still images; however, the current systems are improving and starting to make use of the video cameras to capture a sequence of pictures in order to enhance the authentication process. Perhaps the reduction of video capturing devices prices helped the organisations and systems make use of them [57].

The approaches of face recognition are normally based on the location and shape of the facial features [62]. The features like eyes, eyebrows, nose, lips, chin, and skin colour can be changed during a certain period of time because of aging like wrinkles or surgical operations, moreover, external factors like eyeglasses, lenses, makeup, beards, hair style and colour, and the way the picture was taken including the illumination and angles may also have great effect on the results of the face recognition process. Furthermore, it is preferred that the stored image is three-dimensional (3D) [69], it has been declared that 3D has more advantages in comparison with 2D, the advantages stated by [69] are as follows:

- Improved ability to process face samples acquired from non-frontal angles, increasing viability of surveillance and reducing error rates;

- Improved ability to operate in suboptimal lighting, reducing error rates and environmental restrictions.

Although the advantages seem convincing, there are still some disadvantages with 3D face recognition. They include the need for specialized acquisition devices and processes, and 3D images also require large sample size and processing power [69]. Face recognition is widely accepted; less intrusive, easy to collect, however, it cannot yield a high probability of accuracy in identifying a person when compared to other biometric methods. Therefore, accuracy will be the main reason of restricting the use of face recognition unless improvements on devices to ensure better accuracy take place.

Typing rhythm (Keystroke):

The manners in which different individuals type characters on a keyboard appeared to be different, the term keystroke dynamics was defined by [70] as: “Keystroke dynamics is a technique that monitors a user's fluctuating typing speed patterns” [70]. The typing rhythm or keystroke dynamics determine the time required to press a key, release a key, and pause between a key and another on the keyboard, once this time is recorded, a special algorithm is used to produce a biometric template to be used for future authentication. The main advantage of this type of behavioural biometric is that it does not require any additional hardware device [27], the method requires a keyboard and a computer, which is almost available everywhere.

Voice:

The voice is a behavioural biometric that can be used to identify a person; it is one of the characteristics that differentiate people. Each person has different

speech style and different voice, the invariance of the characteristics of the human speech is due to the dissimilarity of the shape and size of the appendages (vocal tracts, mouth, nasal cavities, lips) in every person [62], which has an influence on the voice of the person. Voice biometrics analyse the inflections of the person's voice [67], to able to collect the voice data, the system requires a microphone and a computer. The system asks the person to speak out one or more sentences into a microphone, this technique is known as text-dependent [57]. By providing different sentences each time, the person can prevent the system from being attacked by a playback of a previous recording of a genuine speech [57], for example, an attacker can record the identification session on a magnetic tape or a digital disk and play it back to the system. Therefore, a different sentence must be spoken each time the person is authenticated to be able to avoid a recorded speech from being played back to the system.

Although the speech of each individual is distinctive, it may not contain enough invariant details to authenticate people on a wide range and for a long period of time [62]. One of the reasons behind this is the person's bodily condition, for example, an illness like cold or flu can affect a person's voice. Another reason is the acquisition device and the environment, in which the first identification session was collected, the quality of the microphone has a great impact on the voice recorded. Furthermore, voice recognition is sensitive to noise, all background noises will affect the voice collected for the identification session, thus, all noises must be filtered.

Like other biometrics voice recognition has its drawbacks such as peoples' emotional and physical state, noise sensitivity, and playback attacks.

Otherwise, it is generally accepted by users and considered to be a friendly way of collecting evidence for authentication purposes in comparison with other biometrics.

Signature:

It is one of the most commonly used identification methods, people use the signature to prove their identity on daily bases, the reason behind using signature as an identification method is because each person has a unique style of handwriting [62]. People sign on personal documents, banking transactions, credit cards and their receipts, legal documents, approval letters, invoices, etc. It has been proved that no two signatures of a person are exactly identical, the emotional and physical status of a human affects the way the signature id made each time [62], [70].

Signature recognition comes in two methods, static (offline) and dynamic (online). The static method is the most commonly used method since ages, the evaluation in the method takes place after the signature is written, because this method relies on the geometric features of the signature [62]. On the other hand, the dynamic method relies on both geometric features and dynamic features, therefore, measurements are made while the signature is being written [62]. In this method, the user writes the signature in a digitised tablet, stylus-operated PDA, a tablet PC, or similar digitised input device [71]. The dynamic method measures features like speed, velocity, acceleration, pressure, time, azimuth, altitude, etc [57]. In comparison with the static method, the dynamic has the advantage of measuring more features while the person is signing and after the

signature has been written, which makes it more difficult for anyone to duplicate other person's signature.

The signature recognition method is accepted by people, and can be easily incorporated into an existing system for identification and authentication purposes [62]. In addition, it is almost not possible to replace any of the elements of a biometric method; however, the signature recognition method is not similar to the other biometric methods because people can change their signature if required. This feature gives the signature recognition a great advantage when compared to other biometric identification methods.

Each identification system has different requirements, specifications, limitations, and levels of security. The selection of the appropriate biometric method for each system depends on number of factors like the user profile, environmental conditions, levels of accuracy required for verification, interoperability, the overall system cost and capabilities, and cultural issues that might affect user acceptance [26], [3]. Table (2) shows a comparison of the biometric types or technologies, with their performance rated against different characteristics.

The biometric technologies have different ratings according to each characteristic, the behavioural biometrics are easy to use and widely accepted by users, but at the same time have number of error incidences that may affect the stability and level of security provided. In contrast, physical biometrics have higher levels of accuracy, at the same time have less user acceptance rates and are more difficult to use.

Characteristic	Fingerprints	Retina	Iris	Hand Geometry	Face	Voice	Signature
Ease of Use	High	Low	Medium	High	Medium	High	High
Error Incidence	Dryness, dirt, age	Glasses	Lighting	Hand injury, age	Lighting, age, glasses, hair	Noise, Sickness	Changing signature
Accuracy	High	Very High	Very High	High	High	High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	High	High
Required Security Level	High	High	Very High	Medium	Medium	Medium	Medium
Long-Term Stability	High	High	High	Medium	Medium	Medium	Medium

Table (2): Comparison of Biometric technologies
Source: [3]

Therefore, the selection of the appropriate biometric technology relies on many factors, mainly on the systems requirements, levels of security, and type of users. According to the factors, the organisations get to choose among the available biometric technologies.

2.2.4.4 Biometrics Advantages and Disadvantages

Biometrics is an authentication method that assures who is gaining access to the system; it authenticates the user not the machine. Therefore, this security method has number of advantages like offering a high level of security and convenience. By using the biometrics method, it is quite easy to check if a person has more than one identity [61], the biometric method is not based off a standard true or false system; it includes levels of security that accept the relative closeness of the characteristic [72]. This security criterion offers good levels of authenticity, integrity, and confidentiality in the identification system.

It is important to mention that the biological features cannot be transferred to another person and at the same time not modifiable [65]. In addition, biometrics cannot be lost, forgotten, guessed, stolen, or shared because they are part of the human's body or a behavioural characteristic in the human that no other person can use [61]. The system extracts the features from the biometric sample and transforms it into templates, a template cannot be used to recreate the original biometric sample provided earlier, it only has details about the user's characteristics [72]. This gives the biometrics method the ability to guarantee information integrity and provide a greater degree of security in comparison with other security methods.

Along with the great benefits that the biometrics method offers, there are number of disadvantages. Every system has its pros and cons, one of the drawbacks of biometrics is not being able to keep biometrics secret, it is public, people can record voices, take pictures, lift fingerprints from anywhere, etc [72]. If the biometric evidence have been stolen or miss used, then it is not possible to replace it [61]. This is a major drawback of biometrics because in some cases and under certain circumstances fake biometrics can be issued, it is quite hard but intruders can go around the system security method and fool the system with fake biometrics. In the case of stolen biometrics, users may want to know what happened and what will happen to their biometric data since it is associated to their identity [72].

As stated by [72], the biometrics technology is costly, not everyone can afford such an advanced security system. For example, iris and retina scanning tend to be a bit more expensive.

Moreover, biometrics scans can cause inconvenience for the user, some types of biometrics are considered to be intrusive, other types require preparation and repetition of scan. The users must be knowledgeable with the scanning devices and educated about the biometric method used in the identification system they are dealing with, they must also accept to use this type biometrics to be able to overcome the inconvenience.

2.3 Smart Card Applications

In order to successfully implement a smart card system it is vital to have the overall know-how of the system and its requirements. In fact, [16] states that the smart card industry can be represented by the following three levels: technologies, core products, and applications. Figure (5) represents these levels:

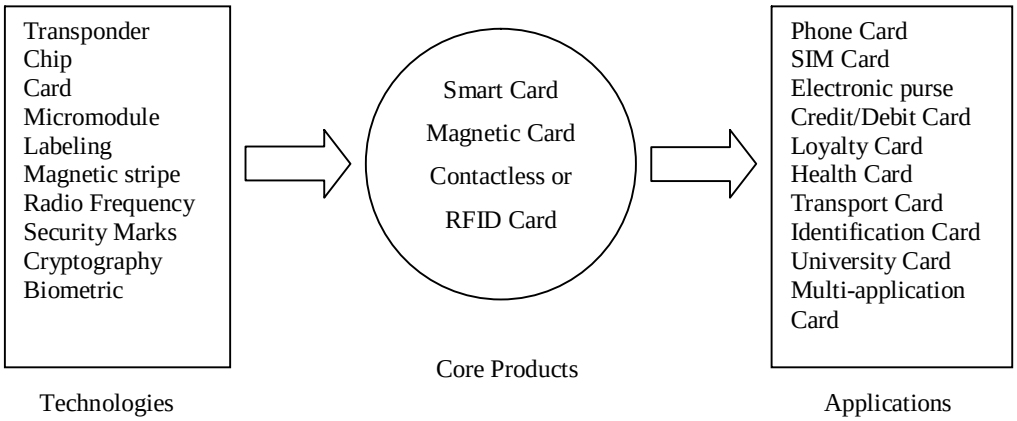

Figure (5): Smart Card Industry levels.
Source: [16]

Using smart cards as a tool to access required confidential information or carry out a financial transaction brings to mind the importance of having the smart card operate in a secure environment. So, it is quite essential to know what each card holds access to, how confidential and private this data is, what

are the consequences and costs of losing this data, how long does it take an intruder to gain access to the data via the smart card, etc.

Various reasons rely behind people committing computer crimes. Card theft or fraud is common these days because simply people have different motivations. “A psychological explanation for fraud would appear simple—greed and dishonesty.” [73]. Some people are just lacking honesty and integrity! This depends on the people’s background, behaviour, and social situation. Others have motivations like curiosity, ego, intelligence, monetary gain, revenge, blackmail, destruction, exploitation, challenge, or competition [74]. All those motivations can somehow lead people to commit card theft or fraud; hence, it is hard to control people’s behaviour or attitude towards using a particular technology. The thing that is achievable is making the smart card users aware of the ways they can help protect their own information in addition to the security methods applied.

It is also crucial to point out the expenditure status of the smart card market during the coming years, as illustrated in figure (6) below; the identity management market expenditure forecast to 2011 will probably reach about 1400 million pounds [2]. This indicates that the market is growing dynamically and the organisations are rushing into using smart cards as a tool to access the required data to their information systems. Also, the graph shows the different types of smart cards used and the other types that are planned to be used in the coming years.

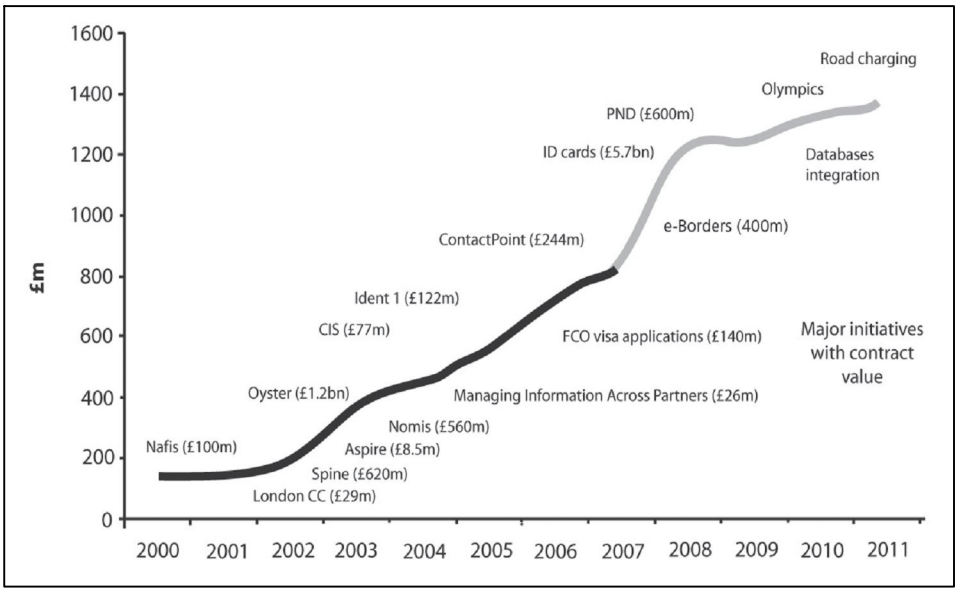

Figure (6): Identity management market expenditure forecast to 2011
Source: [2]

Therefore, a well secured smart card system must be one of the major issues to be looked at. The following chapters of the thesis enclose a demonstration of the smart card applications, the value of data stored in the smart card or accessed through the smart card, the time needed for the user to discover that the card has been lost or stolen, and finally the motivation behind the willingness to attack the smart card system.

2.3.1 Smart Cards in Payment Systems

Smart cards are widely used these days as a payment method; many well known and large banks have explored the significance of smart card technology in payment systems, therefore, transformed their credit and debit cards from magnetic-stripe cards into smart cards. Recently, the use of smart cards with smart card chip reader is being encouraged by the banks as a method of reducing card cloning crimes [75]. In fact, a credit or debit card user has to be knowledgeable of the smart card PIN, and the point of sale (POS) terminal

reading the smart card chip on the card has to verify and authenticate the user for the transaction to successfully take place.

Using the smart cards in payment systems can be classified into three types. They are used as credit cards where payments are made after rendering a service, debit cards where payments are made directly from the account, and electronic purses where payments are made before rendering a service.

It is also significant to mention the EMV specification, which is a product of the joint efforts of three leading card companies Europay, MasterCard, and Visa [27]. The main purpose of this specification is to ensure the compatibility of the cards and card readers, which will allow the consumers to use the three major companies' smart cards interchangeably [76]. This indicates that the EMV specification will provide a common and internationally recognised standard for global interoperability. According to ACI World Wide:

> The majority of financial institutions worldwide that issue credit or debit cards and acquire financial transactions will migrate their existing magnetic stripe cards and transaction processing infrastructures to implement an infrastructure compliant with the EMV standard. [77]

This specification is considered to be a milestone that will affect the future of the smart card usage all around the world.

All those specifications and standards are taking place to facilitate the usage of the smart card technology. Yet, a huge concern still exists, which is credit card, debit card, and e-purse card fraud is a common phenomena. By breaching the system through the smart card the intruder will gain access to the user's account, therefore, uses the user's cash and funds for his/her own benefit. Thus, the smart card holder has to notify the bank or card issuer that the card has

been lost or stolen as soon as possible in order for the bank or the card issuer to cancel the card; otherwise, the thief will start using the card and spending as much money as possible from the card holder's account. The moment the card holder reports the incident, he/she is no longer responsible for unauthorised charges made on their card. The Federal Trade Commission (FTC) states that:

> If you report the loss within two business days after you realize your card is missing, you will not be responsible for more than $50 for unauthorized use. However, if you don't report the loss within two business days after you discover the loss, you could lose up to $500 because of an unauthorized transfer. [78]

Therefore, the card holder has to be careful when using the card, according to the financial institutions law the card holder has maximum 48 hours to report that the card is lost or stolen. This indicates that the intruder needs very little time to gain access to the card holder's account and benefit from the money stored in the account. The card issuer or the bank can support the user only if the user acts as quickly as possible, otherwise, the user will lose his money [78]. As a result, using the smart card as a credit or debit card is a great issue that risks the card holder's most sensitive belonging which is money.

2.3.2 Smart Cards in E-Government Systems (ID Cards)

The expansion of governmental activity to secure and verify citizen identity and at the same time work against identity fraud is a worldwide phenomenon. For the past decade, governments began to implement projects that support chip technology to secure and authenticate citizens as well as achieve other benefits such as improved efficiency and border throughput. Thus, the main purpose behind electronic government (e-government) systems is the ease of access to governmental information and services for citizens, businesses, and government

agencies. The governments believe the using the smart identification card will play a major role in facilitating the e-government activities and communication among all parties.

The identification smart card will support services such as renewing driving licence, viewing birth certificates, various governmental forms, etc [79], [80]. The smart identification card can also support the e-voting technology, which is mainly practicing various election processes through the internet [81]. Furthermore, the smart identification card is considered to be a valid travel document for trips among the countries that allow such use of smart cards and e-gates because it conforms to the international standards for electronic smart cards [80]. As a result, citizens can successfully enter any country in the world that supports e-gate. This is such a huge issue that requires a highly secured system. People with motivations like terrorism or illegal immigration can breach the system and benefit from this technology.

In addition to supporting the previously listed e-government activities, the smart identification card holds various confidential and private data of the card holder, mainly, the citizen. The most common data to be stored in the smart card could be the citizen identification number, name, date of birth, address, personal photograph, occupation, signature, and fingerprint. Additional data could be available to view at the smart card depending on each country government requirements. Some countries have the driving licences, visas, registration certificates, and passport number stored in the identification smart card memory, however, they implement different security level access to these types of information.

Although the reasons behind using the smart identification card is primarily protecting the public, protecting the family, protecting the community, and making life easier [82], the loss or steal of the card will give the intruder the opportunity to access various governmental services including the risk of using the citizen's identity to commit different types of crimes.

2.3.3 Smart Cards in Health Systems

Managing the patient record through an integrated information system has been a great concern for the researchers and practitioners during the past decades; many attempts took place during the past few years to fully computerise the management of patient health record. The aim behind these attempts was to make the patient's health record available across a network to hospitals, surgeries, billing agencies, and health insurance companies. The availability of patient health records across all the concerned parties will contribute to the improvement, ease, and quick delivery of the health care services. According to [83] the fundamental concept behind the health system design is that the patient is the centre of activity for data collection, the system is suppose to be able to provide the answers to the 5 W's (who, what, where, when, and why) together with intervention and service result reports. Therefore, the patient's data must be stored in a multipurpose database and in a retrievable format.

For greatest accuracy of patient data collection procedure, outcome data should be captured as close to the source as possible, including direct data capture from patients themselves and from their families. In order to make maximum use of outcome data [84], systems must be designed to:

1) Store data in multipurpose databases;
2) Share data across different platforms;
3) Link outcome data to other data that might influence or explain outcomes;
4) Allow querying of the data by authorized personnel;
5) Protect patient confidentiality.

These requirements are important for implementing an effective health information system. However, with the increasing demand of providing access to the patient's record anytime, anywhere, and as quickly as possible the smart cards is most probably the best solution. The smart card provides number of benefits such as easy mobility, and storing a good amount of data and information related to the patient. Because of the processing capabilities of the smart card, the development of active programs is effectively designed to easily manage the patient record.

Generally, the smart card gives access to the database that holds record of all the specific details of the patient, through the given access, the required information for the patient could be retrieved. Yet, for quick access to the information the smart card holds number of important information about the patient medical record, it contains information like the patient's personal identification details such as name, surname, identification number, date of birth, place of birth, gender, contact numbers, home and work address, next of kin names and contact numbers, and blood type. It also holds record of the patient's drug allergies, regularly prescribed drugs, immunisations record, and health insurance details.

A study by [85] in Taiwan to investigate the first phase of the national health insurance smart card project stated that the smart card has visible information

and non-visible information. The visible information contains the cardholder's name, identification number, date of birth, photo (optional), and the card serial number (a unique number assigned to each card) [85]. On the other hand, the non-visible information that is stored inside the card can be divided into four segments: basic data, health insurance data, medical data and public health administration data.

The basic data segment stores the identification information for both the cardholder and the card itself [85]. The health insurance data segment contains the cardholder's insurance information and service data for insurance claims. The medical data segment is to record important physician orders, prescriptions and drug allergies. The public health administration data segment contains personal data related to public health such as vaccination records and organ donation notes [85].

As a result, the visible data is mostly about personal identification and the non-visible part contains the patient's medical information and health insurance details. This way of classifying the information that is on the health smart card seems to be the most relevant and effective way. Therefore, having all these details stored on a smart card, in addition to, gaining access to the main database to retrieve full medical reports gives the health smart card a great responsibility of holding seriously confident and sensitive type of information especially when it comes to insurance coverage details.

2.3.4 Smart Cards in Loyalty Systems

One of the modern ways of gaining customer loyalty or even retention to a business today is by issuing the customer an attractive and stylish loyalty smart

card. It is well known that loyalty programs practiced by businesses are mainly used as a competitive weapon in today's huge and competitive business environment; in fact, the main objective that relies behind issuing the customer a loyalty smart card is to improve customer retention and increase spending [86].

Proving to the customer that the business cares about the number of times the customer visited the shop, amount spent during the visits, and type of products and services purchased will result in strengthening the relationship with the customer, therefore, gaining a competitive edge among rivals. However, a study conducted by [87] shows that "When holders are satisfied with the reward scheme of the loyalty card programme, they are more loyal and less price sensitive than unsatisfied card holders" [87]. This indicates that the business must build a rewarding loyalty card programme before the establishment of the loyalty cards. Some businesses start accumulating points from the amount spent by the customer, others accumulate points according to the number of visits, it mainly depends on the type of product or service provided by each business, at the end of the day what matters to the customer is the rewards that are going to be gained after using the loyalty card.

Another main reason behind issuing a customer loyalty card is monitoring and gaining knowledge of the customer's buying behaviour, according to [88] the loyalty cards "provide a clear sign of the great thirst for customer knowledge"[88]. In order for the businesses to acquire such knowledge, they need to collect some personal information from the customer to issue the card and then save the information in the loyalty smart card. The information will most probably be the following [88]:

- Name of the cardholder
- His/her address
- His/her household size
- Date of subscription
- Total number of all shopping visits
- Total amount spent since subscription

Some additional information could be the date of birth and the contact details of the customer like the electronic mail address and telephone numbers. This type of personal information stored in a loyalty smart card may end up having the customer in a risky status if the card has been lost or stolen. Simply, if any one was able to read the information stored in the card through a smart card reader, then thief can introduce himself/herself to the company as if he/she was the real owner of the card and therefore redeems the points collected by the card holder or even buys products and services from the company if the card stores monetary value.

A good example for such a case is the well known loyalty smart card generated by one of the largest stores in the UK, which is Boots advantage card. This card stores the subscribers personal details, in addition to, the accumulated points depending on the amount spent on the store, the customer collects 4 points for each £1 spent in any Boots store all around the UK [89]. Because of the monetary gain that the customer can have while using Boots advantage card, the possibility of losing the card or card theft and having the points redeemed by someone else is high, the reason is mainly the card is not associated with any security method like a password or biometric evidence to proof the identity of the card holder. For example, in [90] a situation where Boots advantage card was

lost is stated. The review says that on a recent visit to Boots the card holder discovered that the advantage card is missing from his wallet. He contacted Boots to be told that his points had been redeemed, this had taken place because there is no ID check on point redemption[90]. It is easy and almost undetectable for dishonest people including the staff to redeem the card holder's points. This example shows how easy it is to benefit from other people loyalty smart cards if the card was not well protected. As a result, even if the smart card does not contain a very valuable amount of information like banking details, it is quite important to have the card holder's information secure to some extent in order to better protect the card holder's privacy and gain his/her trust.

2.3.5 Smart Cards as Prepaid Cards in different systems

The smart cards were used for decades ago as a sort of a prepaid card that contains a small amount of memory, which is used to store phone call units or TV subscription fees. The rapid expansion of smart card as prepaid cards was in Europe due to the huge amount of phone card users [91]. The prepaid smart card was also adopted in the transportation industry; in fact, the UK transport industry realised the real benefits behind adopting the smart card ticketing program and produced the so called London's Oyster cards [92], [93]. The usage of the Oyster cards is not only limited to London's underground network, it also includes buses, it will also be valid on a range of other means of transport including London's Tramlink, Docklands Light Railway (DLR) and certain rail routes [94], [95]. The fact that the prepaid transport card is reusable made it more flexible to use. The card has the ability of holding credit or so called subscription rights, details of the card holder, and access to a range of services

and applications [91]. The reason behind making it a reusable card that is capable of storing high-value and low-value ticketing details is the believe that the smart card is a safe way of storing data, where the data cannot be copied or altered because of the high security methods that are accompanied with the implementation and usage of the prepaid smart card [91].

On the other hand, because of the monetary value the card holds it must now make its way and stand against attacks. Attackers will be motivated to get access to the smart card contents to benefit from the data stored within the card. Thus, users of prepaid smart cards must take into account that their cards are attracting attackers and therefore use them carefully.

It is also important to mention that transport smart card has been utilised in studies that are concerned about the travellers' behaviour [96], [92]. Every time the card is used the transactions are recorded to monitor the card holder's behaviour [96]. Therefore, the card does attract researchers and analysts to conduct their studies depending on the information the card provides while the card holder has not a single idea that the card is contributing in a study. This issue raises the confidentiality of the transport card user, which is a very sensitive issue.

Chapter 3

Risk Management

This chapter is concerned about the Risk Management Programme that is carried out to examine the smart card system security. Risk analysis is based on identifying the smart card system assets and their values, identifying threats and the possible attacks, identifying the vulnerabilities of the system, producing a security requirements list, determining the risks associated with the usage of the system, and finally suggesting risk mitigation and controls to better safeguard the smart card system assets and users.

The primary data will mainly be collected from articles related to the study subject that are published in engineering and scientific journals, and interviews with representatives and experts that work in a smart card employed environment. On the other hand, secondary data will include written materials such as the governments' publications, relevant documents, and organisations communications (e-mails, web sites, and newspapers).

3.1 Managing the Smart Card System Security

In order to effectively manage an information system, it is important to apply a risk management program to be able to avoid negative impacts on the system along with reducing the risks to an acceptable level. The overall objective of this study is to assist the organisations and governments that are involved in this

system to better manage risks that have harmful impact and are more probable to happen.

The risk management encompasses three main processes: risk assessment, risk mitigation, and evaluation [97], [98]. Risk analysis is the process of assets identification, threats recognition, vulnerabilities identification, and risk determination. Whereas risk mitigation is achieved by applying the required safeguards [97]. Evaluation is the continuous process of evaluating and implementing a successful risk management program.

3.1.1 Asset Identification and Value

The assets of any smart card system are similar to most e-business information systems. They basically consist of Hardware, Software, System and User Interfaces, Data and Information, People, and Web and Security Services. An asset is only an asset if it holds some value to the system [99], so table (3) will show each asset and the value it holds to the system.

Any harm that may affect these assets will have a negative impact on the smart card system, along with all system users. Therefore, assets of the system must be protected against any type of attacks. Protecting the information that is saved within the smart card system components like smart cards, servers, and databases, in addition to balancing and protecting the electronic transmissions of information over the networks is an essential task to be taken into consideration.

Asset	Value
Hardware	System equipment (PCs, workstations, servers, card readers, biometric readers, etc), staff access points, networks like internet and intranet connections, data and information storage (smart cards and databases, and system backup.
Software	Operating systems, information security (anti-virus and spyware programs), database software, compilers, utilities, and applications.
System and User Interface	Direct interaction with system and web services, and access to mobile devices like the smart card and viewing its contents.
Data and Information	User personal record, account numbers and details, amount saved (monetary value), biometric template, user digital signature, private and public key, or passwords.
People	Performance, development, control, management, customer confidence and trust, and communication.
Web and Security Services	Provide interface to the e-business platform, government or banking transactions (certificate requesting, forms, statements, any other documents), collaboration with other business parties (e-mail), publications, news, generating passwords, exchanging cryptographic keys, etc.

Table (3): Smart Card Information System Assets and their Values.

3.1.2 Threat Identification

It is important to be familiar with the threats that may affect the system. A threat is the potential for a particular threat source to practice vulnerability [99]; threats are the possible means by which a security policy may be breached [12]. A threat source can be any person, thing, event, or idea that poses danger to an asset within a system in terms of confidentiality, integrity, availability, or legitimate use. Moreover, threats can be deliberate or accidental [12]. If it was accidental, then the responsible attacker has done it by mistake and meant no

harm. In contrast, if it was deliberate, then it can be categorised as a passive threat such as network sniffing or it can be active such as negligence, errors, attempt to gain unauthorised access to the system, or changing the value of a particular transaction by malicious persons. Therefore, possible threats on the smart card system can be [12], [99], [97], [98]:

- Unauthorised system access,
- Hacking and System intrusion,
- Information leakage or theft,
- Integrity violation (errors and omissions by insiders or outsiders),
- Availability violation like Distributed Denial of Service (DOS),
- Illegitimate use (dishonest or disgruntled insiders or outsiders),
- System penetration and tampering.

Threat sources have different motivations that may lead to carrying out various attacks on any governmental or business information system; therefore, the parties involved in the smart card system must be familiar with the human threat environments and their different motivations. Moreover, being aware of the possible threats and threat sources will help the smart card system administrators and analysts create an efficient security requirements list that will facilitate the determination of the risks that might take place.

3.1.3 Attacks on the Smart Card

Security is a huge matter; it tackles every single stage of a product's lifecycle. The security of the smart card must be considered in early stages, starting from the development stage, the manufacturing stage, ending up with card in use stage. The main reason behind taking into consideration the security issue in all stages is the possibility of attacking the smart card at any stage.

3.1.3.1 Attacks during the Development Stage and Manufacturing Stage

According to [24], attacks can take place at the development stage of the smart card. During the development of the hardware of the smart card microcontroller, a small number of people carry out the development within a secured and monitored facilities, in addition, the computer systems that are used for the design of the microcontroller are connected through an independent network that is highly secure where no outsider can have access. Hence, the attack on this stage may possibly come from an insider. The comprehensive knowledge required to affect the security of the chip in a negative way by an outsider is rare, therefore, such an attack is highly unlikely to occur unless an insider turns out to be an attacker.

On the other hand, the development of the smart card software including the operating system is another concern to be looked at. The origin of the software used must be determined, otherwise it is prohibited [24]. The main purpose of knowing the origin of the software in use as stated by [24] is to decrease the possibility of manipulating the development tool, which might have the intention of changing the generated program tool.

Furthermore, [24] declared that it is quite essential to have strict authentication during the manufacturing stage of the smart card or chips, although is it a closed environment, the access is closely controlled, and each access is recorded, the manufacturing stage must be monitored from a security viewpoint because some technically interesting and effective attacks can be carried out here by an insider.

3.1.3.2 Attacks during Smart Card Use

During this stage, access to the smart card is easier than the previous stages, simply because the smart card is not in an independent highly secure environment where few people are monitored while working and equipments are highly secured, now it is used by users in more opened networks, this raises the probability of a successful attack.

Attacks during the smart card use stage can be physical or logical [24], the physical attacks manipulate the area of semiconductors usually, in contrast, the logical attacks do not attack the hardware properties directly, it is more focused on the communication and flow of information between the smart card and the terminal [24].

The following is an overview of the common physical attacks that threat the smart card security, physical attacks require number of equipments like microscopes, laser cutters, micromanipulators, focused ion beams, etc [100]. In addition to the corresponding knowledge of their applications that are only available to few specialists or organisations [24]. However, this does not mean that a potential attacker will not be able to commit such an attack; therefore, the protective mechanisms must be applied to the smart card and its microprocessor.

Invasive Attacks

Invasive attacks are attacks that function by physically gaining access to the microprocessor embedded in a smart card, they require the microprocessor to be removed and directly tampered [100], [101]. They tend to damage the appearance of the smart card, so there is no possibility of reusing the original smart card again. In theory, this type of attacks compromise any security

measure of any microprocessor, they require expensive equipments, high expertise, and great investment in time to produce results [101]. Invasive attacks involve reverse engineering and physical probing on buses and memory.

- **Reverse engineering:** target the internal design of a chip to be able to identify the given chip or block functions [101]. Trying to reverse engineer secure blocks, obtaining information that can improve the knowledge of chip design, finding a weakness in the chip, and attempting to read the contents of the Read Only Memory (ROM) is the attacker's main objective. The attacker reveals the chip by removing the plastic body of the card and removing the gold plate, then using fuming nitric acid or acetone to remove the resin used to protect the chip. The next step is identifying the different functions by observing the chip under a microscope [101]. Successful reverse engineering attacks will result in loss of proprietary asset, compromising the chip's integrity, and gaining a competitive advantage by knowing the other product's information if the attacker was a company [100], [101]. A good example of a recent successful reverse engineering attack on smart cards is the attack on MIFARE Classic chip. Is has been declared by [102] that the security of embedded devices usually relies on the secrecy of proprietary cryptographic algorithms. However, these algorithms and their weaknesses are disclosed by reverse engineering, this is what happened to the MIFARE Classic chip where the proprietary cryptographic algorithm used was reverse engineered and then broken. This successful attack allowed the attacker to get hold of the secret key used in MIFARE Classic chip.

- **Physical probing on buses and memory:** another method of invasive attacks on the microprocessor is placing a probe on the bus lines, the bus lines are long metal tracks that carry data including cryptographic keys and other secret values between the parts of the chip [103]. It is quite hard to make direct contact with the bus lines because they are fabricated in the lower layers of the chip. Although the chip is packaged inside a protective coating, once it has been removed from the packaging, identification of the bus lines and their contents can be done using an oscilloscope [100], [103]. An attacker can also use an optical microscope to examine the layers of the chip [101], the images can be extended using a specific technique to stain the ROM [103], which holds the operating system and its related data and code, in addition, it may hold the applications of the smart card. So, by observing the ROM, an attacker can gain secret information.

Side-Channel Attacks

These types of attacks are considered to be non-invasive attacks because they take place on a working smart card chip, so they do not require the destruction of the smart card most of the time [101]. Side-channel attacks consist of observing a side channel while the information is being processed, the attacker seeks to obtain secret data like cryptographic keys or PINs by observing how the characteristics of a smart card change while processing different information [100], [103]. The types of side-channel attacks include timing analysis, the data exchanged on the I/O channels, power analysis, the electromagnetic emission, or any other effect of the computation [101].

- **Timing Analysis:** it is considered the simplest side channel attack when compared to the other attacks. Mainly, this attack consists of observing how long a given process takes to execute and draw a conclusion from these observations [100]. The time required to complete a specific process can leak information about the data being processed, for example, the digits of a PIN are checked byte by byte, and a negative result returned when a wrong digit is encountered, therefore, an attacker can use this information to determine how many digits of a guessed PIN are correct [100]. At present, PIN comparison is changed, it is constructed in a way that all digits of a PIN are always compared, so there is no difference in time between positive and negative comparison results [101]. However, observing the times difference and producing timing tables may still leak some relevant details of what type of data is being processed.
- **Power Analysis:** this side channel attack is the most common against smart cards, these attacks attempt to use variations in some measurable characteristic of a smart card to be able to determine secret data like cryptographic keys or PINs [103]. Power analyses are measured by observing the power consumption of the smart card chip with an oscilloscope. Because of the simple structure of the smart card chip, the internal processes along with the data processed make it possible to have measurable and interpretable effects from the power consumption [24]. There are two main types of power analyses; these are Simple Power Analysis (SPA) and Differential Power Analysis (DPA). As explained by [24], [100], and [101], SPA is about observing the power consumption of a

smart card chip over time, by using an analogue-digital converter to determine the voltage change at a resistor connected in series at a high temporal resolution. The amount of power consumed is dependent on the type of instruction being executed and the data being processed, simply, the same program sequence with the same data results in a certain cycle of power consumption of the processor, running different data leads to different power consumption. For example, [100] explained that the power consumption during the implementation of AES consists of nine identical rounds and a tenth shorter round, the encrypted data is decrypted using a secret key, the power consumption varies depending on the value of a secret key, therefore, an attacker can obtain the secret key values by inspecting the power consumption even if the difference is relatively small [104]. In comparison with SPDA, DPA is about conducting a statistical analysis to discover even smaller differences in the power consumption of the chip as described in [104] and [105]. The power consumption during the processing of known data is determined first, then during the unknown data, the measuring is repeated many times, after that, the mean value is calculated to eliminate noise, after all the difference is determined and therefore the unknown data can be figured out [24]. In fact, this attack allows the attacker to break a secret key into smaller portions that can be analysed separately. Therefore, power analysis on smart cards has serious impact on hardware and software, which makes it extremely important to apply the suitable countermeasures.

- **Electromagnetic Analysis:** this is a complicated attack to implement, electromagnetic analysis measures the electromagnetic radiation of the chip, conclusions can be drawn about the internal sequence of events in the smart card chip, the measurement information collected in this type of analysis is similar to DPA [24]. This attack requires the chip surface to be exposed to be able to get a strong signal and therefore deduce information [101]. Superconducting quantum interference devices can be used in order to measure magnetic fields of low extension strength [24]. Furthermore, the signals obtained in electromagnetic analysis can be processed in the same way as power analysis, analysis can be done individually or treated statistically [101]. However, the technical effort along with the necessary knowledge required is generally not available, which makes it a hard attack to take place compared with the previously mentioned attacks.
- **Fault Induction Attacks:** it is one of the side-channel attacks that attempt to inject a fault during the normal functioning of a smart card and hope that this fault will result in exploiting secret data [101]. These type of attacks allow information leakage on the cryptographic key that is being used, they have been working successfully with both public key and private key algorithms [106]. The most common fault injection techniques stated by [106] are variations in supply voltage, variation in the external clock, temperature variations until the chip exceeds the threshold's bound, light exposure, laser over an exposed chip surface, or x-rays and ion beams radiation on the chip. An abnormal signal sent to the smart cart may result in an unusual response [100], therefore, an attacker can have the advantage

of attempting to avoid sensors by illuminating certain portions of a chip. The effects from fault injection attacks vary, depending on which part of the chip being attacked; however, the main countermeasure to avoid this type of attacks on smart cards is redundancy.

Other important types of attacks while the smart card is in use are the logical attacks or so called software attacks. Attackers can write malicious software, which can be employed in a software attack on a smart card, for example, in smart cards that support Java Card it is possible to load and run software. The following are the possible logical attacks.

Bug exploits

To be able to bug or manipulate the data in a smart card during a session, a good example by [101] was to place an error in a loop test, which makes it hard to detect, or some read/write operations would result in an obvious vulnerability. It is quite hard to discover a bug in a deployed smart card, but once it is discovered it may be possible to perform illegal operations [101]. Another example is bugging of the data transmission stated by [24], an electrically insulated dummy contact is attached to the I/O interface of a smart card, therefore, the original I/O interface will no longer be connected electrically. The dummy contact along with the original contact are then connected to a fast computer, which can cut out or insert any data while the terminal and the smart card are communicating. If the computer was fast enough, then the smart card and the terminal will not be able to find any difference between the normal data and the manipulated one.

Illegal bytecode

This is another way of attacking smart cards that support Java Card, it is called illegal bytecode or ill-formed applications [101]. These attacks are malicious applications that do not have valid bytecode parameters or made of illegal sequences of bytecode instructions. The bytecode is a complex process and bytecode verification is difficult, the smart card processors are not fast enough to be able to run the verification, also, the standard algorithm requires a memory that is beyond the smart card's ability [101]. Therefore, the attacker can retrieve details or even execute functions and take full control of the smart card.

Attacks during PIN comparison

Attacks during the comparison process of a PIN can be carried out; it focuses on all the methods related to the data sent to the smart card in order to be compared with the stored value or template. For example, power analysis can be practised during the PIN comparison process [24], a drop in voltage at a resistor connected to the Vcc circuit will make it possible to determine through power measuring whether the retry counter was increased or not, this command must be sent to the smart card together with the comparison data. In this case, if a positive comparison was returned before the retry counter was increased, then the comparison value could be determined by an attacker [24]. Another possible attack during the PIN comparison could be through run-time optimisation, which is called time analysis [24]. The corresponding comparison routine carries out a byte-by-byte comparison between the entered and saved PIN, if the routine is programmed in a way that a difference in the comparison of two PINs will result in an immediate abort of the routine, then this will result in minimal run-

time differences that can be measured with suitable equipment, and therefore simply used by an attacker to determine the secret PIN.

3.1.3.3 Attacks on Biometrics

Attacks on Biometrics are growing because the use of Biometrics as an authentication method has become more widespread. The most dangerous threat against Biometrics consists of the acquisition of the employed Biometric data or its corresponding templates by unauthorised parties. A study conducted by [107] showed eight possible vulnerable points that can be identified in a biometric authentication system, it showed the system modules along with the channels interconnecting them. An attacker can steal, modify, or delete the data exchanged among the biometric system modules through the weak points demonstrated in figure (7).

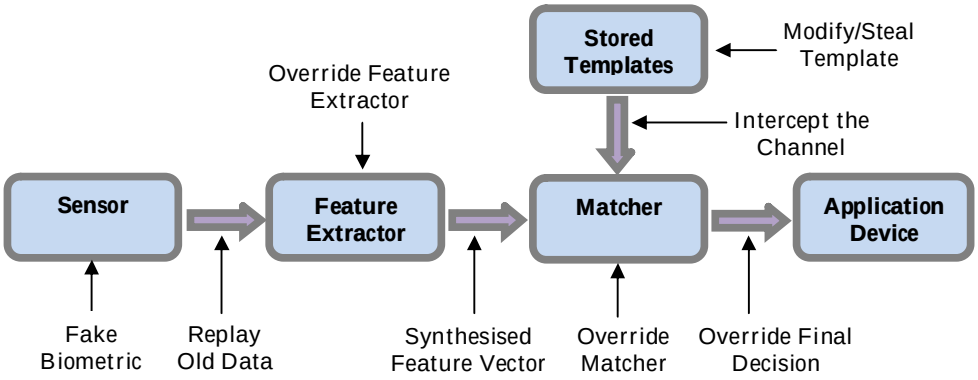

Figure (7): Eight vulnerable points in a general Biometric System.
Source: [107]

Therefore, understanding the weak points, and being aware of the nature and risks of attacks on Biometrics is imperative to researchers, designers, and system developers. A study by [108] discussed the attacks and vectors of

Biometrics. The following are the attacks and weak points explained by [108], [109], [110], [111]:

Fake Biometrics

Spoofing or presenting a fake biometric to the sensor in order to get access to the system. This may be as simple as presenting a picture to a face recognition scanner or as difficult as producing a fake fingerprint out of the original finger by using the biometric traces left by the owner. Physical fake biometrics are likely to take place when using fingerprints, hand geometry, or face recognition schemes. Other digital fake biometrics attacks such as obtaining the templates or digital images stored are likely to take place inside the biometrics system, where the attacker requires access to the biometrics system in the first place.

Replay old Data

In this case, the presented biometric data is captured and replayed. This can happen by submitting a previously stored biometric signal, such as a recorded audio signal, to the feature extractor bypassing the sensor.

Override Feature Extractor

This attack targets the feature extractor normal practice; the data processed is maliciously altered and manipulated in order to produce templates with preselected features, for example using a Trojan Horse attack. Then again, other possible way is to attack the software of the biometric system in order to disable it through practicing a DOS attack.

Synthesised Feature Vector

Usually, the extractor and matcher components are combined. In the case where the two components are separated and communicate with each other

through a network, there is a possibility that a third party intrudes the communication channel and alters the templates before they reach the matcher, an example of this type of attack is called “hill climbing” and is described in detail by [112] as follows:

> A hill-climbing attack may be performed by an application that sends random templates to the system, which are perturbed iteratively. The application reads the output match score and continues with the perturbed template only when the matching score increases until the decision threshold is exceeded [112].

Therefore, this attack injects a stream of fake biometrics into the system to fool the matcher, to be able to practice the attack successfully; the attacker must have access to the biometric system communication channels and the match scores.

Override Matcher

This attack replaces the matching scores that are produced by the matcher with fake ones, possibly by a Trojan Horse. The important thing to mention in this attack is that the authorised users will not notice any difference because the system will continue providing them access.

Modify/Steal Template

Altering or stealing a template that is stored in the biometric system by attacking the storage area, the templates are stored in a database, a smart card, or the biometric reader in some systems. The result of the attack will either deny legitimate users from having access to the system or allow illegitimate users to access the system.

Intercept the Channel

The templates that are stored in the system travel in a communication channel between the storage areas like a database to the matcher. An attacker can intercept the communication channel and alter or manipulate the templates while being transmitted through the channel before reaching the matcher.

Override Final Decision

It is a form of a bypass attack where an attacker can block the final decision or insert a new one. Injecting a false acceptance between the system and the end device will result in accept/accept for all cases, therefore the final decision is going to be overridden.

The previously explained framework by [107] is a good point to start from, it simplifies the task on the system analysts. By looking at the framework, the analyst will have a clear idea of the weak points that are vulnerable to successful attacks. Yet, the framework is considered to be abstract when it comes to identifying vulnerabilities of a biometric system in a holistic view. To add extra interpretation to the framework a study conducted by [113] focused on the technical testing of the biometric devices. It proposed a framework that includes the vulnerable points of [107], in addition, it identified five extra subsystems: data collection, signal processing, transmission, data storage, and decision, allowing a more clear analysis of the potential attack points.

After that, [110] added to the previous frameworks. The extended framework in [110] added three more components: administrative supervision, underlying information technology environment, and token presentation. Figure (8) shows the framework produced by [110]. There are twenty demonstrated attack points

in the biometric system, and twenty two vulnerabilities identified. This is an indicator that attacks possibility on biometric systems is something that needs to be reduced when employing a biometric system. There are some countermeasures to the attacks presented in the framework that are mentioned by [108] like liveness detection, randomising input biometric data, using multiple biometrics, clearing retention of data especially in the sensor area, emphasising on the usage of strong cryptography and digital signatures, physical security, and network security.

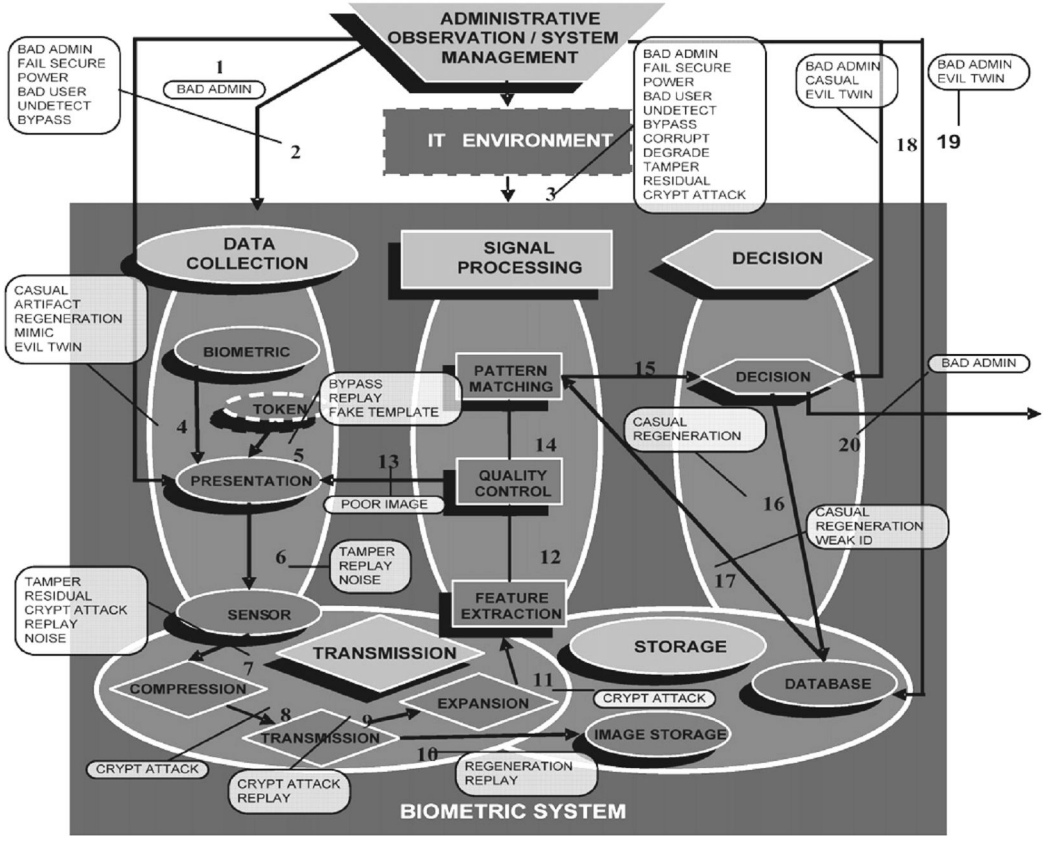

Figure (8): Bartlow and Cukic framework presenting the Biometric System Vulnerabilities. **Source:** [108].

These defences will enhance the biometric system and will add strength to it; however, it does only reduce the probability of successful attack but it does not eliminate the attacks from taking place.

Accordingly, the governments and organisations must study and review the history of the system break-ins and security violation reports, also, they must conduct interviews with the system administrators to be able to identify the latest potential human threats. As a result, the governments and organisations will be able to produce, and at the same time make available to all users, a threat statement or list that contains the threat sources and the potential threats along with the common frequent attacks, which will exploit the system vulnerabilities.

3.1.4 Vulnerability Identification

"The security system is only as strong as its weakest link!" [114]. Thus, for the system to be stronger and well protected from any internal or external harm, the system administrators must test their system and find its weaknesses, which are the system's vulnerabilities. Vulnerabilities are weaknesses that may potentially be exploited to cause loss or harm, they are the susceptibility of a system to threats; it is an aspect of a system that leaves it open to attack [99].

Therefore, after identifying the threats and attacks that may harm the system, the next step the governments and organisations must do is to test the system and discover the possible system vulnerabilities that can be exploited by potential threat sources. The following are some common technical and non-technical system vulnerabilities to be taken into consideration [99]:

Technical Vulnerabilities

- TCP/IP protocol stack
- Lack of database backup
- Weak user authentication and authorisation methods

- Old encryption methods
- Firewall allows inbound telnet, and guest ID is enabled on the organisation's server

Non-technical Vulnerabilities

- Negligence in removing the terminated employees' system identifiers
- Carelessness of monitoring employees' behaviour

To be able to avoid the previous common system vulnerabilities, the government and organisation managers and administrators must review previous system auditing and assessment documentation, evaluate the system security test reports, update the system vulnerabilities list, and benefit from vendor advisors.

3.1.5 Development of Security Requirements List

This step is about developing the security requirements list for the smart card information system, the main reason behind developing this list is to assess the sensitivity of the system and to determine the security requirement for each system phase because each phase in the system is accompanied with different security requirements. The awareness of the possible threats and attacks that may harm the system and its' users, in addition to identifying the system vulnerabilities before developing the security requirements list will facilitate the development of an effective list.

Every information system has the following main security goals [4]: confidentiality, integrity, non-repudiation, availability, authentication, and authorisation.

Confidentiality simply means that a message should not be read by other than the sender and the intended recipient [97]. According to the smart card system, private data like the health record, criminal record, immigration details, must be kept private from being disclosed to unauthorised individuals, entities, or even processes. Loss of confidentiality may lead to jeopardising national security, loss of public trust, or even legal action against the responsible party.

Integrity means that the sender and receiver want to be sure that they both have exactly the same message [12], [99], [97]. This means the integrity is the ability to protect data from being altered or even destroyed in some cases by intentional or accidental manner. Therefore, violation of the smart card system integrity will be the bridge for successful attacks against the system, which will result in inaccuracy and fraud.

Non-repudiation is defined as the ability to limit parties from disproving that a transaction took place [12], [99]. The individuals cannot deny that they were involved in the transaction; this can be achieved by signatures.

Availability is mainly making the system resources and facilities obtainable and accessible to all system users [97], [4]. This security requirement prevents and detects the improper denial of access to the services provided by the smart card system. Loss of availability in the smart card system will lead to less performance and will reduce the productive time. It may also delay some important governmental activities that will have negative impact on both providers and users.

The recipient wants assurance about the identity of the sender, hence, the process of one entity verifying that another entity is who they claim to be is

called authentication. The smart card system has to apply trusted techniques to ensure efficient authentication of the system components, most familiar techniques of authentication are passwords and signatures. Loss of authentication means that system is not anymore confident and is vulnerable to any type of attack.

Authorisation means that access to data should be permitted only to authorised users; it is the process that ensures that a person or a program has the right to access certain system resources [12]. This process may vary; every user in the smart card system has certain resources to be able to have access to. However, other security goals may be required according to each application or during different system phases such as anonymity, public trust, logging, etc.

It is preferable that the governments and organisations sort out the security requirements in the smart card system in terms of the service phase and user type. Each application contains the following phases [115]: System set up, which is mainly setting up the system hardware and software. Verification, this phase is where the employment of the appropriate mechanisms for authenticating all system users is required. Providing the service, this phase is about offering the service online to the end users. After service, this is the last phase of the system; it is responsible of maintaining the progress of the offered service, providing the end user with the output of the transaction (certificate, form, statement, update, etc), and system storage.

E-Banking, e-gates, e-health, e-voting, e-purse, and other online public services:

Service Phase	User	Type of Security Requirement
System set up	Administrators	Availability
Verification	Operators Smart Card Users	Authentication Authorisation
Providing the service	Smart Card Users	Confidentiality Integrity Non-repudiation Availability Logging (not applied for e-voting) (anonymity and untracability for e-voting only)
After service	Operators	Logging

Table (4): Service phases and the related types of security requirements.

The information listed in Table (4) is derived from discussions with a smart card expert [116], who is working in an organisation that produces and manages smart identification cards. Table (4) shows that there is a distinction of the security requirements per service phase. All the security requirements are important to ensure the overall system security, but assigning different security requirements to specific service phases will help the system management create a better security policy for the smart card system adopted. To be able to develop and maintain the security requirement list, awareness of the possible threats, attacks, and vulnerabilities is essential.

During the system set up phase, the administrators of the system must ensure that the system is going to be available to all users, specify access privileges, and support the functionality required. Hence, they have to protect the system from possible threats and attacks that violate availability mainly Distributed Denial of Service (DOS), as explained previously in the thesis.
The second service phase involves the verification of the system operators and users, which requires the employment of security mechanisms that allow authorisation and authentication to legitimate users to access the system like

PINs, Passwords, or Biometrics. It is vital to take into consideration the fact that there are possible threats like unauthorised system access and hacking, in addition to different physical and non-physical attacks on the employed mechanisms that are mentioned in sections 3.1.3.2 and 3.1.3.3, which can harm the system users and violate the authentication and authorisation security requirements. Applying the most appropriate authentication mechanism at this service phase is quite important and is not an easy job to handle, especially with all the possible threats and attacks that may take place.

During providing the service phase, which involves the users of the smart card system, numbers of security requirements have to be ensured because this phase is a critical phase with great number of transactions and users exchanging information. The confidentiality (non-disclosure) and integrity (non-modification) of the information exchanged among the users and the providers has to be obtained. In addition, maintaining non-repudiation and proof of origin while the transactions are taking place among users is crucial. Also, time stamping and logging are important to handle possible arguments and disagreements that might occur among system users and providers. Many information and details are exchanged in this phase, so protection against threats and attacks is a priority. For example, the threat sources of violating integrity can be insiders or outsiders, the same can happen with violating confidentiality. Successful attacks on the smart card and the security mechanisms employed will violate more than one security requirement of the system at the same time, for example, as mentioned in section 3.1.3.2, an attacker can get hold of the legitimate user private key through practicing a successful physical attack on the smart card,

this will result in violating the confidentiality, integrity, and non-repudiation security requirements.

The final service phase is the operators' responsibility, they have to ensure that the users are satisfied and their logging activities are saved. Being aware of the system vulnerabilities will help the operators avoid information loss and leakage, in addition, backing up the output of the transactions and information exchanged is very important to avoid problems with the system users.
Hence, assigning the security requirements to each service phase will enhance the management of the smart card system security and will provide a flexible and expandable list that can be used to better serve the system users and help the system administrators determine the risks that might take place in each service phase.

3.1.6 Risk Determination

The purpose of this step is to determine the risk that may face the information system and to assess the risk level (high, medium, or low) [97]. Risk is the measure of the possibility of security breaches and the potential severity of the resulting damage, on other words; it is the measure of the cost of vulnerability taking into account the probability of a successful attack [12], [99], [97]. The risk is considered to be high if the value of a vulnerable asset is high and the probability of a successful attack by a particular threat source is also high. Therefore, to be able to determine the risk level, it is recommended to have a Risk-Level Matrix [98]. By using the Risk-Level Matrix, it is possible to detect the possible risks associated with the system and at the same time determining the level of each risk.

However, examples of the risks that are associated to the system are [97]:

- Natural disasters,
- User error (accidentally delete, overwrite, or insert wrong number),
- Loss of money, data, or information,
- Computer Crimes,
- Hardware Crash or Software failure,
- Database or Server failure.

Therefore, the governments and organisations have to take the risk assessment seriously and include it in their monthly tasks in order to avoid and eliminate possible risks from taking place. Emphasis must be on the adequacy of the existing security controls to eliminate or at least reduce the risks.

As mentioned earlier in the chapter, the risk management program consists of three main processes, the processes are: risk assessment, risk mitigation, and evaluation. Based on that, the next step is to assess and determine the risk that might occur when the smart card system is employed. Risk analysis determines the risk level and examines the risk probability and impact associated with each type of smart card. Therefore, a qualitative risk analysis approach is applied to determine and analyse the risk that is accompanied with each type of smart card, the reason behind applying a qualitative approach is because in this case it is not possible to quantify the system threats and vulnerabilities to be able to come up with quantified risk levels. It is more effective to use a risk matrix to determine the risk levels. This section explains the qualitative risk analysis approach and shows the study results.

One way of determining the risk associated with the employment of a particular technology in an information system is using a risk matrix [117]. The

level of risk is measured by a risk value; this value could be described as high, medium, or low, however, other scales could be applied depending on each case. Thus, this study will use the following risk scales:

Risk Level	Description
Unacceptable	This risk must be mitigated directly with certain controls to an undesirable risk level or even less within a specified short period of time, the sooner the better.
Undesirable	Should be mitigated with certain controls to an acceptable risk within a specified period of time but could take longer period than the unacceptable risk.
Acceptable with controls	Should be verified that procedures or controls are in place.
Acceptable as it is	No mitigation required.

Table (5): Risk levels

The risk level is determined based on the assessment of the likelihood of occurrence of the unwanted incident and its consequence or sometimes called impact in terms of loss of asset value [118]. The likelihood of occurrence or in some cases called the probability of happening is mainly stating how likely the event is to occur, the probability should be a number between 0-1, which is most probably represented as a ratio of the number of chances by which an event or an unwanted incident may happen [118], for example a 40% chance for an event to happen. On the other hand, the consequence states the severity of the event and what losses or damage to the system are going to take place; this is also represented as a ratio.

So, the qualitative way of analysing the risk involves assessing the likelihood and impact of an unwanted incident to be able to determine the level of risk. The risk matrix is also a likelihood / consequences matrix; it mainly shows the ranges

of both the likelihood of occurrence and the consequences, each range is listed on one side of the matrix or on an axis. The likelihood of occurrence is described as follows [119]:

Likelihood (Probability)	Description
Frequent	Can be experienced in a continuous manner.
Probable	Will occur several times.
Occasional	Unlikely but possible to occur.
Improbable	So unlikely to occur, but possible.

Table (6): Likelihood of occurrence or probability levels

Then again, on the other side of the risk matrix the range of consequences severity is listed, it is described as follows [119]:

Consequences (Impact)	Description
Catastrophic	Very high severity perhaps whole system failure.
Critical	High impact with huge losses.
Marginal	Medium impact with ability to recover.
Negligible	Low impact but might cause small damage.

Table (7): Consequences levels

Therefore, the risk matrix is formed of the probability axis and the consequence axis. The intersection of the likelihood of occurrence of an attack with the impact of the attack will identify the risk level of each unwanted incident that might take place and harm the information system; it also maintains an awareness of the risks throughout the lifetime of an information system.

Based on the data collected from the primary and secondary sources of the study, risk analysis is carried out. Depending on each type of smart card, which could be an identification card, banking card, loyalty card, health services card,

or prepaid card there are number of factors in determining the probability of attacks occurring and the impact of these attacks are considered, therefore ending up determining the level of risk that is related to each type of smart card.

The factors that are examined in this study are cost, time, motivation, and amount of information stored in each type of smart card. The following are number of figures and tables that illustrate each factor in comparison with each type of smart card. The second step is developing a risk matrix that shows the risk tolerability depending on the probability of attack taking place and the consequence of this attack on each type of smart card.

The cost is related to the monetary value that the card possibly store or have access to. Card fraud losses has been a great issue to the payments industry, according to APACS, the fraud facts report produced in 2009 stated that the annual card fraud losses in the UK-issued cards are increasing. The fraud types on plastic cards are different; table (8) will show the fraud types and the total monetary value losses in the years 2003-2008:

*All figures are in £ millions

Fraud Type	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**
Card-not-present	122.1	150.8	183.2	212.7	290.5	328.4
Counterfeit	110.6	129.7	96.8	98.6	144.3	169.8
Lost/Stolen	112.4	114.5	89.0	68.5	56.2	54.1
Card ID Theft	30.2	36.9	30.5	31.9	34.1	47.4
Mail non-receipt	45.1	72.9	40.0	15.4	10.2	10.2
Total	**420.4**	**420.4**	**504.8**	**427.0**	**535.2**	**609.9**

Table (8): Fraud Losses on UK-Issued Cards 2003-2008
Source: [120]

Table (8) shows that the money figures have increased from £420.4 million to £609.9 million within a range of five years. In essence that, the smart cards have

been introduced and used in the market approximately three years ago, it did not contribute to making the fraud losses figures decrease.

Figure (9) illustrates the relationship between the type of smart card and the cost of losing the card or an intruder having access to the card contents, the monetary data in figure (9) are anecdotal. It is based on an assumption of the most probable amount of money that each smart card could possibly have access to. Figure (9) shows that the cost related to the identification card is very high comparing to other types; the reason is that the ID card gives the attacker access to many privileges.

The attacker will have the ability to claim to a bank, hospital, government agency, or any other entities that he/she is the legitimate user of the card, which will result in high losses of monetary value and other personal information. The banking card is also causing loss of relatively high amount of money when comparing to the other types of cards.

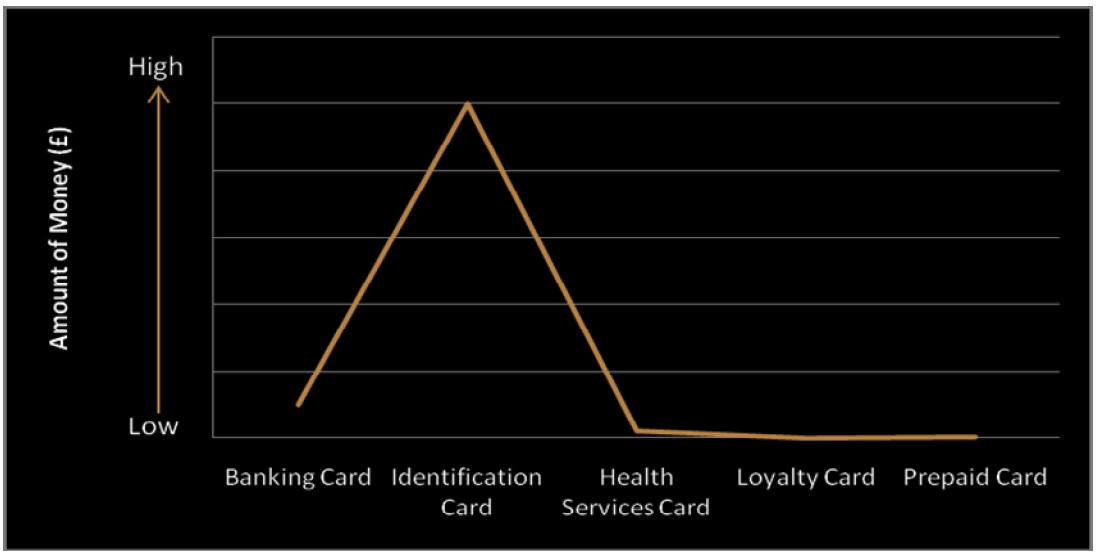

Figure (9): Type of Smart Card compared to the Cost factor
Source: [120] and [121].

The banking card allows the attacker to get hold of the amount of money stored in the account or accounts that are linked to the card, so depending on each type of customer, the amount will be in thousands as an average. The health services card can have a great impact on its card holder as well, especially if it was linked to the health insurance party, according to [121] about 1.5 million Americans have been pointed out as victims of medical identity theft with losses of approximately $20,000 per victim. This amount of loss indicates that the health services card can give the attacker access to a huge number of benefits. The rest of the card types contain fewer amounts of money stored, which can be limited to few hundreds of pounds and therefore costing very little damage in case of theft or loss.

The time required for the smart card user to realise that the card has been lost or stolen is an important issue to be looked at. By pointing out the time the user needs to discover the disappearance of the card, it is essential to mention that each type of smart card has different timing. The user needs less time for example one or maximum two days to realise that the banking card has disappeared because people use their banking cards almost on daily basis, in addition, the banks allow the user to inform the bank of the loss of the card within maximum 48 hours, otherwise the bank is not anymore responsible of defending and supporting the card holder.

On the other hand, the health services card has the maximum days comparing to the other types of cards because the user will look for the health services card the next time he/she has to visit the health care centre or hospital, which might require few days or few weeks. The number of days is based on

anecdotal evidences that depend on the users' behaviour when using a smart card. Thus, mainly the banking card along with the identification card need less time for the user to discover about their loss.

Table (9) shows the motivation behind the willingness to attack the smart card and gain access to the information stored within, the determination of the type of motivation is based on the outcomes from interviews conducted with analysts from organisations that employ smart cards [116] and [122].

Smart Card Type	Banking Card	ID Card	Health Card	Loyalty Card	Prepaid Card
Monetary Gain	✓			✓	✓
Destruction of information	✓	✓	✓	✓	✓
Illegal information disclosure	✓	✓	✓		
Unauthorised data alteration	✓	✓	✓	✓	✓
Blackmail	✓	✓			
Destruction	✓	✓	✓	✓	✓
Exploitation	✓	✓	✓	✓	✓
Revenge	✓	✓		✓	✓
Challenge	✓	✓	✓	✓	✓
Ego	✓	✓	✓	✓	✓
Rebellion	✓	✓			
Curiosity	✓	✓	✓	✓	✓
Intelligence	✓	✓	✓	✓	✓
Unintentional errors and omissions	✓	✓	✓	✓	✓
Competitive advantage and espionage	✓	✓	✓	✓	✓

Table (9): Smart Card Types Compared to Motivation Factor

Depending on the applications that the smart card supports and the type of data stored within the card, the attacker will be inspired. The motivation will be greater when the gain behind getting hold of the data is greater. It is clear that if the card contains or has access to more monetary value, then the motivation behind attacking is going to be very high. The reason that attackers have less motivation attacking the other types of smart cards is because the level of benefit is relatively low in comparison with the identification card and banking card.

Banking Card	ID Card	Health Card	Loyalty Card	Prepaid Card
- Title - Forenames - Surname - Issue Date - Expiry Date - Issue No. - Account No. - Card No. - Signature - Security Code - PIN/Password	- Title - Forenames - Surname - Date of Birth - Place of Birth - Address - Gender - Marital Status - Nationality - ID Number - Personal Photo - Occupation - Signature - Blood Group - Biometric Image - Vision and Disability - Driving License Number - Driving License Date - Driving License Type - Card Barcode - Expiry Date	- Title - Forenames - Surname - Date of Birth - Place of Birth - Address - Gender - ID Number - Personal Photo - Marital Status - Number of Kids - Next of Kin - Contact numbers - Blood Group - Health Record - Drugs Allergy - Drugs Prescriptions - Immunisations - Health Insurance	- Title - Forenames - Surname - Date of Birth - Address - E-mail Address - Contact Numbers - Household Size - Accumulated Points - Shopping Behaviour - PIN/Password	- Title - Forenames - Surname - Date of Birth - Address - E-mail Address - Contact Numbers - Personal Photo - Monetary Value - Tickets - Password - User Uni ID - User Uni Name - Expiry Date

Table (10): Smart Card Types Compared to Amount of Information Factor

Table (10) shows the amount of data stored on each type of smart card; this is determined from conducting personal communication with representatives from different organisations that employ smart cards [116], [122], and [123]. The reason behind creating this table is to encapsulate the data to construct the UML diagrams in page 118.

Loyalty and prepaid cards have a less important and at the same time low amount of information stored on the smart card in comparison with the other types. However, banking card has access to a very huge and sensitive amount of information especially money, in addition to a very sensitive amount of data stored in the smart card itself, which must not be available to anybody other than the card holder and the related bank.

The identification card contains even more sensitive data stored within the card chip; it could also contain monetary value in the case of the card supporting e-purse. The identification card also allows access to the system; it exchanges data and information to and from the system. Hence, the identification smart card has access, stores the most sensitive information, and has the biggest amount of information comparing to the other types of smart cards.

An element impact schedule that is developed by [124], suggests that there are five key elements that need to be assessed to determine the relative criticality or impact of failure on systems when conducting risk analysis. The elements are time criticality, health and safety, customer satisfaction, embarrassment, and financial. The loss impact table and the information classification table are presented in Appendix (A), the elements and their assigned levels of impact are listed, to be able to assign impact levels on each

type of smart cards, data and information are obtained from [125], [126], [127], [128], [129], [130], [131]. To be able to summarise the impact of each factor on each type of smart card, table (11) is produced, where some elements are derived from [124]. By observing the impact of the factors and elements on the different types of smart cards illustrated in table (11), the outcome shows that the severity of impact on the banking and identification cards is higher in comparison with the rest types of cards.

Factors and Elements	Banking Card	ID Card	Health Card	Loyalty Card	Prepaid Card
Financial Loss	Very High	High	Medium	Very Low	Medium
Amount of Information and Information Sensitivity	High	Very High	Medium	Low	Low
Motivation	Very High	High	Medium	Low	Medium
Time Sensitivity	High	High	Low	Low	Medium
Customer Satisfaction	Very High	Very High	Medium	Low	Low
Embarrassment	Very High	Very High	Medium	Medium	Medium

Table (11): Factors and Elements Impact on Smart Cards

The next step is to develop a risk matrix to point out the risk level associated with the employment of each type of smart card. Based on the outcomes illustrated in tables (8), (9), (10), (11) and figure (9), in addition to the judgements made by the interviewees [116], [122], and [123] while collecting the primary data of the study, the risk matrix is developed. In order to construct the risk matrix, the likelihood of occurrence and the consequence of any attack to the smart card must be considered.

Therefore, taking into account the previous factors and their relationship with each type of smart card, the probability of attacks (Pa) on each type of smart card along with the consequence of attacks (Ca) are going to be assigned. Table (12) shows the weights and their descriptions:

Weights	Probability of attack (Pa)	Consequence of attack (Ca)
0 to 0.2	Improbable	Negligible
0.3 to 0.5	Occasional	Marginal
0.6 to 0.8	Probable	Critical
0.9 and above	Frequent	Catastrophic

Table (12): Probability of attack and Consequence of attack weights

Thus, weights are assigned to the smart card types to determine the risk level. The main purpose of developing the risk matrix is to show the risk tolerability level that each smart card type has. To be able to distinguish between the different levels of risk in the matrix, different colours are assigned to each risk zone as suggested by [132] and [119]. Figure (10) is the risk matrix that demonstrates the types of smart cards along with their risk levels.

The matrix shows that the loyalty and prepaid smart cards have an acceptable level of risk because of the small probability of an attack to take place, plus the low impact of the attack because these types of cards have less sensitive data and information stored comparing to the other types of cards, hence, even if one attack or more took place, the smart card system will be able to handle the risk because the value of the stored data is manageable and losses are able to be recovered.

Moreover, the health services card mainly contains the patient's personal details plus the health record; sometimes it is also connected to the insurance company that will cover the patient's bills. Thus, the health services card is placed on the acceptable risk with controls zone, which indicates that any attack to the smart card will result in marginal consequences that could be taken care of if controls were significantly applied to the whole information system, that will

happen if the employed safeguards are efficient and the system backup and recovery scheme is effective.

Figure (10): Risk Matrix

Furthermore, the matrix shows that the banking card is within an undesirable risk zone and it is probable for attacks to take place. The consequences of the attacks will have critical results on the system and the users. This is simply because this type of card has access to and contains very sensitive data, which is basically money. Attackers will increase the effort of

trying to attack this type of smart card because the results will be rewarding. So, it is quite risky to use the smart card as a banking card unless more security is applied to shift the card from this risk level to an acceptable level with controls.

The identification card has a marginal impact on the system and the users in the case of an attack occurring. The likelihood of attacking this type of smart card is probable because the attacker will gain a great amount of details, will get access to governmental facilities and services, and many other benefits that were listed earlier.

Finally, the most risky type of smart cards is undoubtedly the identification smart card that is equipped with access to the users' banking accounts. This type of card contains great amount of details stored in addition to the possibility of monetary values if it supports e-purse or linked to users' banking accounts. Motivations are very high behind trying to attack this type of card, and the probability of attacking is considered to be frequent plus the impact of any attack will result in severe damage. Although this type of card will facilitate the daily transactions and will add value to the e-government system, it is yet very risky to use because the failure of this type of card will end up in causing very great damage to the e-government system. Gaining the trust of the users and ensuring the safety of their most sensitive and private data is not a simple task.

Therefore, extra care and effort are required to try to shift the identification smart card with access to banking accounts to a better risk level zone, to be able to encourage users to use the card and ensure their information safety. Employing sophisticated security methods to this type of card is essential,

however, taking into consideration the availability and usability of the employed methods is also critical.

As a result, the risk matrix showed the types of smart cards and the associated risk to each type of smart card, which will play a role in guiding and helping the information system developers build up a special security configuration that is relevant to each type of smart card.

3.1.7 Risk Mitigation

It is extremely important to mitigate or even trying to eliminate the risks. The main idea behind this part of the process is to come up with controls to eliminate the risk or reduce the level of risk to an acceptable level. As a matter of fact, the elimination of all risks is almost impossible [12], [97]; therefore, it is the responsibility of the governments and organisations management to employ the most appropriate controls to the smart card system to decrease the impact of risks to an acceptable level. Usually, security controls are derived and configured to protect against the given threats from the previous threat identification step. The security controls contain number of measures like system architectures, engineering disciplines, and security packages [97]. The goal of all these measures is to satisfy the security requirements and to secure the whole system contents.

The security controls at the smart card system can be divided into identification and verification, cryptographic key management, security administration, and system recovery. According to the risk matrix produced previously, it is important to suggest the required security controls and safeguards to each type of smart card system. By putting together the outcomes

and suggestions from the interviews with experts, analysts, and technicians, of different smart card systems, in addition to the final output of the risk matrix presented earlier, suggestions of the required security controls and safeguards are set. Figure (11) demonstrates each smart card system and its required controls and safeguards. Based on the risk level associated to each type of smart card, the security methods presented in figure (11) are suggested.

Banking and ID smart cards are within the marginal and critical impact area where the risks are undesirable, therefore they require advanced and robust authentication methods to make sure that the user is who he/she claims to be, both PIN and Biometrics have to be implemented, or even a combination of Biometrics methods can be implemented together to be able to offer higher authentication, moreover, they require a powerful cryptographic key management scheme like PKI to enhance the system security.

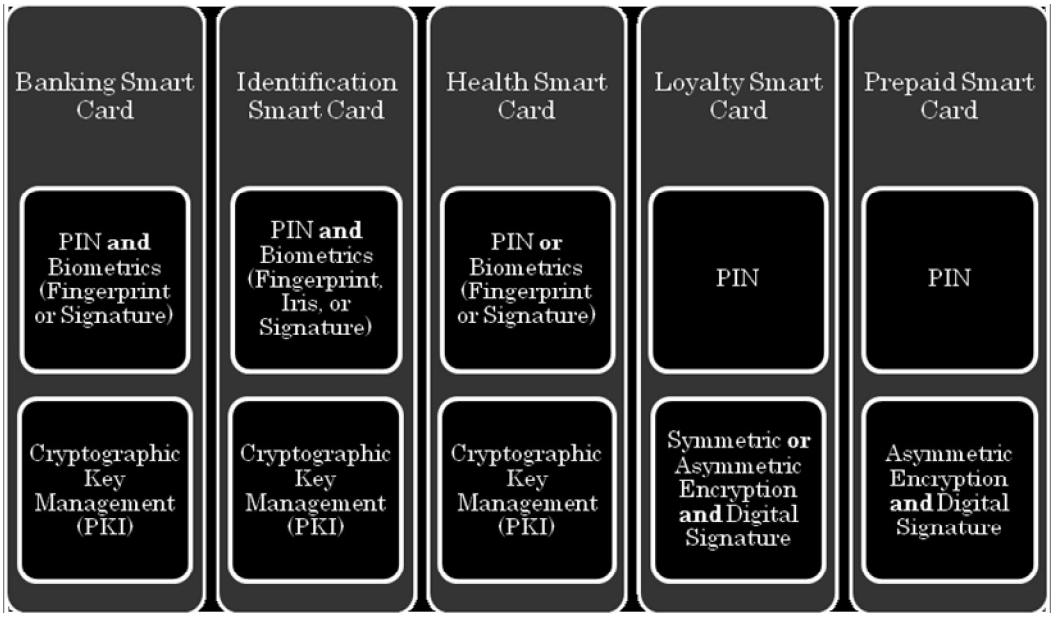

Figure (11): Security Methods suggested to each type of Smart Card System.
Source: [116], [122], and [123]

The Health smart card can have either PIN or Biometrics to ensure better authentication of the users, in addition to a good cryptographic key management scheme like PKI. Finally, the Prepaid and Loyalty smart cards are within the acceptable level of risk zone, therefore, there is no reason for implementing very strong and expensive authentication and cryptographic key management schemes.

Having a general smart card design that is applied to all smart card systems regardless of what the system serves sounds ineffective and perhaps costly for no reason. It would be a better idea if the smart card is designed and equipped with the relevant elements and security methods depending on what the smart card stores and what functions are employed in the system.

3.2 Concluding Remarks

Risk Analysis is a significant management technique that allows the smart card system administrators and operators to evaluate the system security, having an effective risk analysis process will facilitate the management of the controls and safeguards that the system requires. Knowing the possible threats, exploiting the system weak points, and determining the possible risks will enhance the decision making process of the system management, will help meeting and securing the customers or end users needs, and will reduce the possibility of implementing unnecessary controls and safeguards or vice versa.

Now that the smart card system assets and their related values are presented, it is much easier to know what are the controls and safeguards responsible of securing. Moreover, the security list allows the administrators to

focus on what security objectives need to be met, in addition to what type of users are involved in each phase, this is quite essential to monitor the system performance.

The qualitative risk analysis method used in this study made is subjective in nature; however, it provided an easy way to understand and express the risks associated with each type of smart card. It also provided sufficient identification of problem areas. For example, it showed that the identification smart card contains huge number of information stored within the chip, which increases the risk of losing very sensitive and confidential information in case of an attack occurring.

The qualitative risk matrix made it easier to point out the impact and likelihood of risks that might take place in the smart card system. Consider the difficulty of determining the impact of the smart card server going down under the quantitative method, in contrast, it is much more easy to make the system administrators agree that the impact would be a major loss, critical loss, or even a minor loss. Hence, the chosen way of determining the risks showed a clear and efficient outcome. By producing the risk matrix, it is now possible to declare that each type of smart card faces different types of risk with different likelihood of occurrence and different severity of impact. Therefore, it is not a good idea to generalise that any smart card system has to employ a very robust and expensive security measures. This will make the organisation implement unnecessary security controls and safeguards in some cases; on the other hand, some systems really require strong authentication methods and high levels of

cryptography and key management techniques but may employ weak controls and safeguards.

As a result, the risk analysis process gave a detailed explanation of the threats, attacks, vulnerabilities, and risks and related to the smart card system as a whole, and gave specific risk levels associated to the different smart card systems along with the required security methods that are appropriate to each type of smart card, which achieves part of the study objectives that are listed in the beginning of the thesis.

This chapter explained the smart card system assets and the required security list that includes the main security objectives like confidentiality, integrity, authentication, availability, and non-repudiation. These results are the main input of modelling the smart card system components and protocols in chapter (4). In addition, this chapter discussed the threats, attacks and vulnerabilities of the smart card system regardless of the smart card type used, which is going to be the input of modelling the attacks in chapter (5).

Chapter 4

Smart Card System Modelling and Design

In this chapter, a brief review of the modelling languages and their different uses is discussed. Next, the current and the proposed smart card systems are modelled using different types of UML diagrams such as use case, class, and sequence diagrams. The last part of the chapter discusses the concluding remarks of the models and designs of the smart card system.

4.1 Modelling Languages Related Work

Security protocols are set of rules that are designed to make sure that the data transfer among the system parties achieves all the security goals; however, designing and implementing these protocols remain difficult and possible to fail against different attacks. To be able to effectively integrate the security protocols within the systems early development stages, modelling languages and techniques are used to better visualise the entire system components.

There are different modelling languages that can be used to model security protocols with different styles. One is the Communicating Sequential Processes (CSP), which is a process algebra that is used to describe and analyse security properties and protocols by providing a mathematical framework [133], this method is able to provide an expressive framework that shows the exchange of messages among agents. However, to be able to use CSP, the designer must have

specialised knowledge and training mainly in mathematics, which limits the usage of this method to specialised people.

GSPML presented by [134], is a visual security protocol modelling language that provides a visual modelling language suitable for the security specific problem of protocol modelling. It is quite impressive; yet, this language introduces new notations and complex models that are targeted to security specialists and is not easy to be understood by others.

The UML is the modelling language that is used to produce the models in this study; it includes several types of diagrams that represent different parts of a system, some model the static structure of the system and others model the dynamic behaviour of the system entities [135]. To support using UML for secure systems development, an extension in form of a UML profile using the standard UML extension mechanisms called UMLsec is given by [136], [137]. UMLsec uses a combination of use-case driven process with a goal directed approach, the three main mechanisms of the extension are stereotypes, tags, and constraints [138].

Stereotypes and tags are used to create and present the security requirements and assumptions, constraints may be attached but they should be satisfied by modelling elements with the related stereotype [137]. An adversary can be created in UMLsec to be able to model possible threats on a system, the adversary model is created with certain capabilities depending on the considered level of strength for the adversary and the physical properties of the system designed, the adversary can read, insert, or delete parts of the system when the attack takes place [137].

UMLsec was used to indicate possible vulnerabilities on Common Electronic Purse Specifications (CEPS) [136], it was also used to define security permissions that enforce restrictions on the workflows of a system [139], and other systems that are related to security development. The following sections include the smart card system design and modelling.

4.2 Analysing the Smart Card System using UML

After showing the risks associated with using each type of smart card, it is important to look for a more secure and less risky way of employing the smart card system. This is the part of the risk management programme that deals with risk mitigation. As listed previously in the thesis, there are number of methods that are used in today's digital era to ensure the system security and user privacy, however, each method has its pros and cons. A robust and secure smart card system requires a design that ensures the implementation of a perfect selection of policies, procedures, architecture, technology, and staff. In order for the electronic commerce to be a complete success, the implementation of solid security methods and indisputable user identification techniques are required to take place.

Therefore, the issue here focuses on two dimensions, the first dimension is to employ security methods that secure the system as a whole including the system access points, storing and transmitting information, system components, system networks, etc. The second dimension is to focus on employing the best and most accurate user identification and verification techniques to solve the problem of user privacy allowing the user to operate in a more confident and secure

environment. Practically, physical or digital attacks to any system are carried out by people, which points out the importance of accurately identifying the people who should have access to the system and keep track of their behaviours.

Through focusing on those two dimensions and employing these security requirements the risk mitigation phase of the risk management programme will achieve its goals. However, it must be taken into consideration that there is no existing system that is 100% secure, no matter what is done to operate securely in any digital or computerised system there will be a way somehow to breach the system. That certainly does not stop electronic and computer specialists from coming up with the best mechanisms to keep their systems secure.

Furthermore, the smart card system is one of the sensitive information systems these days; it has the same requirements of any computerised system in addition to the great emphasis on system security, user privacy, and information confidentiality. To have a better idea of the smart card system and its components, operations, applications, data and information, and security mechanisms the following UML diagrams were created to illustrate the smart cards system.

4.2.1 Overview of the Smart Card System

Figure (12) is a use case diagram that gives an overview of the basic components and functions of any smart card system. The Actors illustrated in figure (12) represent the main components of the system, which are the User, Smart Card, Smart Card Reader, Client, Server, and Database. The use cases represent the functions or services that take place while the system is operating.

The focus of the analysis in this study will be on the functions of three main components, which are the User, Smart Card, and the Smart Card Reader.

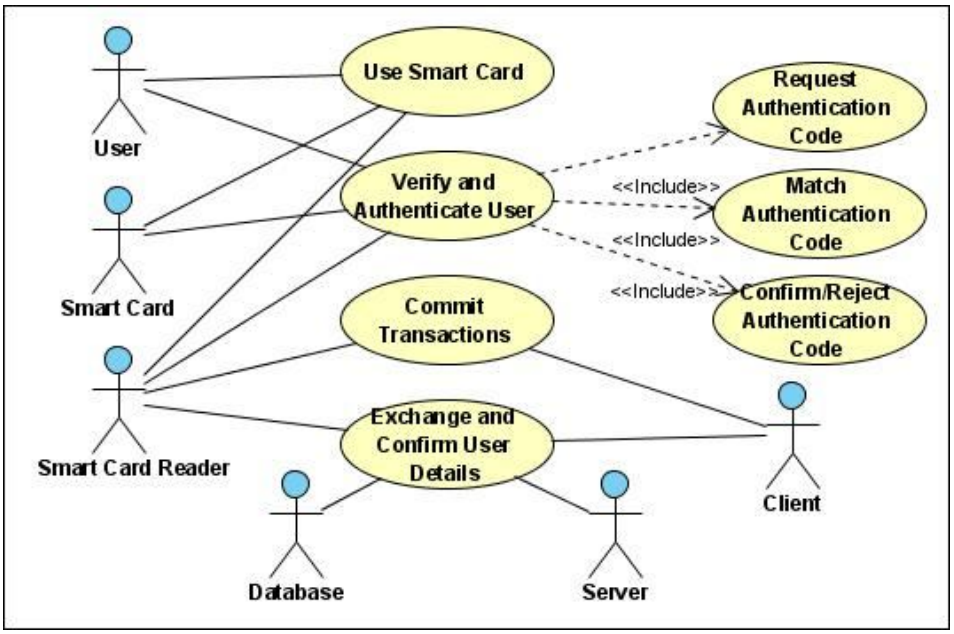

Figure (12): Use Case Diagram- Overview of the Smart Card System

When the User decides to use the Smart Card, the first step is inserting the Smart Card in the Smart Card Reader that is provided by the smart card system. The Smart Card Reader has number of jobs to take care of, it has to verify and authenticate the User and Smart Card, commit transactions, and exchange and confirm the User details with the other system components.

- The first function is verifying and authenticating the User and the Smart Card, which includes number of sub functions. The Smart Card Reader requests the authentication code from the user; this code can be a user name and password, PIN, or biometrics. Then, it compares the provided code with the code stored in the Smart Card, if the matching process is true then it authenticates the User and Smart Card and allows access to the

system, otherwise it rejects the request and cancels the transaction, therefore, not allowing the User to get access to the system.

- The second function is communicating with the system components Client, Server, and Database to retrieve the User details that were stored within the system during the enrolment process. Then the details are sent to the Client to carry out the next function along with the Smart Card Reader.
- The third function is committing the transaction that is requested by the User. This function requires communication between the Smart Card Reader and the Client. The Client shows the transaction details, and the User details that are retrieved from the system Database. Then it commits the transaction, exchanges details with the Smart Card Reader, and finally sends a confirmation to the Smart Card Reader.

Basically, this is what happens when a user gets involved in a smart card system. No matter what type of smart card was used or how complicated or simple the system was, these functions will take place. By having a closer look at each use case illustrated in the diagram, it will be clear that there are number of functions included within each use case, which need to be stated precisely to better study the smart card system, and to be able to come up with some proposed solutions related to the system security and user privacy.

Moreover, the smart card system sensitivity, system security, and user privacy requirements depend on the services the system offers and the type of smart card used in the system. Smart cards are employed in various information systems like payment systems, personal identification systems, loyalty systems, etc. Therefore, smart cards are equipped with different applications,

specifications, security mechanisms, and data in each type of information system.

4.2.2 The Amount of Data stored in each Smart Card Type

According to the type of the information system the smart card serves, the amount of data stored within the smart card varies. The class diagram presented in this section demonstrates the smart card system components and shows specifically the different types of smart cards used in today's digital environment along with their contents. The reason behind creating the smart card system class diagram was to describe the system structure by illustrating the system components, their attributes and operations, and their relationships between each other.

The key point in this diagram is to show the amount of data that is stored within each type of smart card and the operations that are performed by each type of smart card. The User can own one or more smart cards depending on what systems the user is engaged in. Obviously, the User is the main source of the original personal data; on the other hand, the User details that are stored in the Smart Card and the system Database are extracted from the user during the registration or enrolment phase. The User's role in the smart card system is to insert the Smart Card into the Smart Card Reader, request a transaction from the system, scan the Smart Card if the Reader has a touch pad, scan biometrics if the Reader has a biometric pad, or insert PIN if the Reader has a key pad.

There is also a possibility of signing a document or a biometric pad if the system requires extra evidence or confirmation. Regardless of the type, the Smart Card stores the user data, system data, and the security data like

templates, keys, algorithms, etc. It represents one of the main components of the system; therefore, the study is concerned about the data stored within the card and the flow of this data throughout the whole system. The Smart Card has the capability of reading, writing, saving, and updating data. It has direct communication with the other system components especially the User and the Smart Card Reader, and can also confirm the transactions that take place within the smart card system.

The most important thing behind using the Smart Card is enhancing the security of the system, the question that arises here is: Does it really enhance the system security or does it represent a weakness in the system if it was misused? The answer to this question is never certain. Any component of any computerised system that is misused will make the system vulnerable to any kind of an attack, and therefore increase the probability of risks occurrence. However, if the Smart Card was built and controlled in a way where it loses its access to the system in case it was breached, that will make the Smart Card one of the best choices in terms of securing the data of the current information systems.

This is a very hard goal to achieve; it is not as easy as it sounds. An important thing to point out at this stage is the amount of data that is stored within each type of Smart Card. The class diagram in figure (13) specifically shows the amount and type of data stored in the smart cards.

- **Loyalty Smart Card:** it has the least amount of details stored, also, there are no monetary values stored in the card, so the need for sophisticated security mechanisms to be employed is not a great concern for the loyalty

system owners. Chip and PIN is the security method that is the most probably employed mechanism in the loyalty smart card systems.

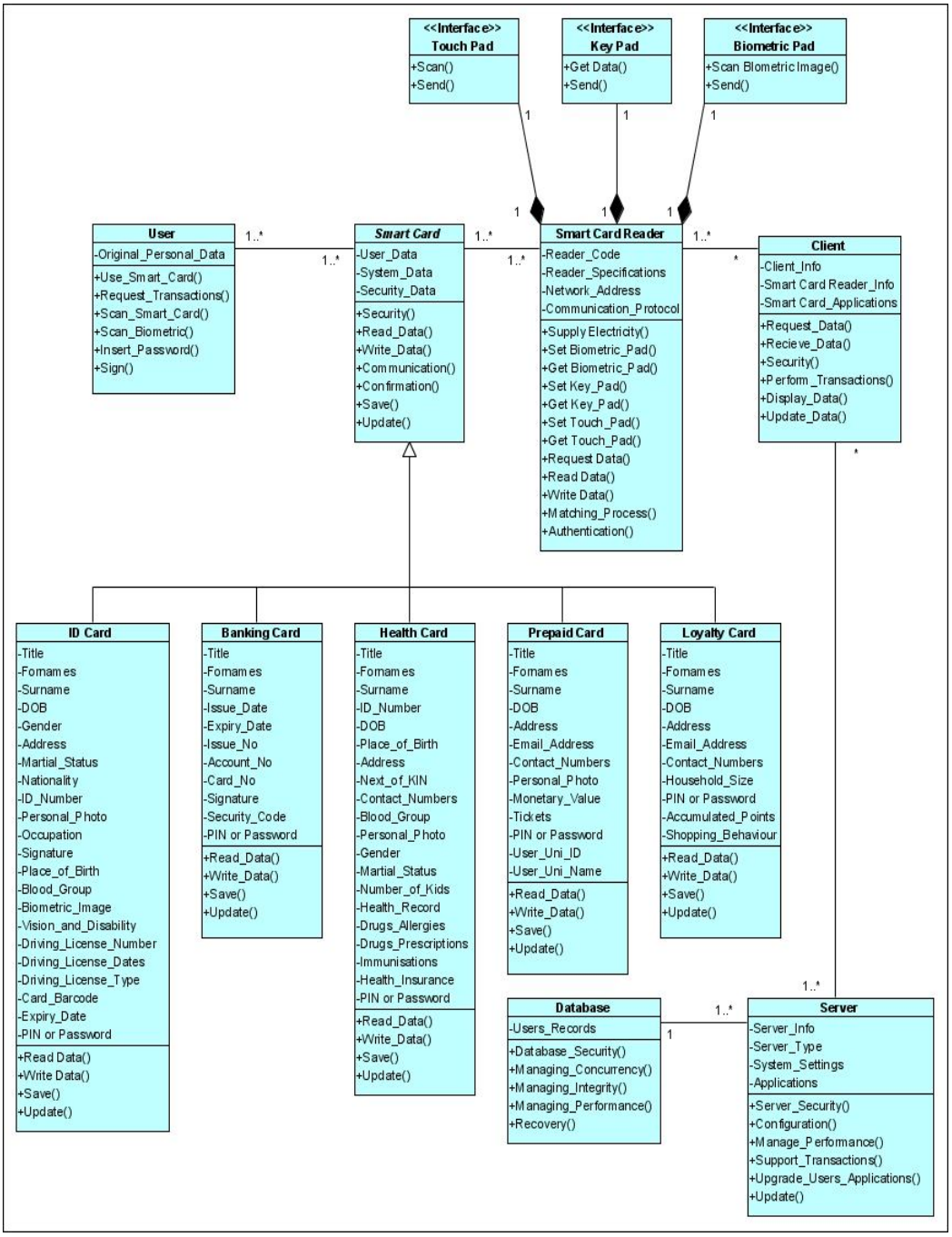

Figure (13): Class Diagram- The Amount of Data Stored in Each Type of Smart Card

- **Prepaid Smart Card:** it contains more details than the Loyalty Smart Card; the most important difference is the monetary value and the extra User

identity details that are stored within the card. A good example would be the Oyster transport card that is used in London, the news about the breaches in the security of the MIFARE chip that is used by the Oyster card was publicly revealed. As reported in [102], [140], the discoveries of Karsten Nohl from University of Virginia and Henryk Plotz who effectively publicly revealed much of the cryptographic architecture at the core of the MIFARE Classic chip have been reported, in addition, the work of the digital security group at Radboud University in the Netherlands who continued with where Noel and Plotz left off was revealed. There work showed that there can be no doubt that both teams had cracked the MIFARE Crypto-1 algorithms, and the Radboud team was travelling freely in London Underground, which without a doubt means that the data stored within the smart card is vulnerable. This indicates that the intruders can have access to the sensitive data that is stored within the Prepaid Smart Card, therefore, have the ability to use the data in committing different types of attacks to the system and User ending up causing harm to all system components. Thus, is it really worth it to store all those details in a Prepaid Smart Card? This is what the system designers need to think about.

- **Health Smart Card**: it is very similar to the ID Smart Card; it contains all the User personal details plus contacts names and numbers in case of an emergency, health record, drugs allergies and prescriptions, and immunisations. So, this card here contains more sensitive data than the previous ones except that the Health Smart Card does not hold any monetary value. When it holds access to any kind of health insurance

programme where the User can pay for his medical expenses through the smart card, then the smart card holds access to extra sensitive data that deals with monetary issues. This will result in increasing the probability of attacks on the card and therefore increasing the risks that are associated with using this type of smart card. Information leakage from this type of smart card will harm the User privacy especially the confidential records related to his/her health and medical status. The User reputation will be affected depending on his/her role in the society, if the User was a well known personality in any community, then attackers will be more concerned about the User's private and confidential data.

- **ID Smart Card:** the same or even more can happen to the User ID Smart Card, this type of smart card holds the hugest amount of details that are stored within the smart card comparing to the other types of smart cards. The class diagram shows that the ID Smart Card basically holds all the identification elements of the User including very specific details like blood group, disabilities, signature and biometrics, and driving licence details. The huge amount of details stored within the ID Smart Card increases the chance of attackers committing attacks to get hold of the User details. Simply because getting hold of these details without the User knowing allows the attackers to pretend to be the User in order to steal money or get other benefits, this will make the User suffer from serious and various consequences that may take place because of the attackers actions, this type of crime is known as identity theft, which is very popular and is the main reason behind attacking ID Smart Cards.

- **Banking Smart Card:** is more attractive to attackers in comparison to the other types of smart cards because of its access to monetary values. It holds the User's identification details plus the User's account details like account number, issue and expiry dates, security code, and PIN or password. In fact, the worst case scenario is to combine the ID smart Card with the Banking Smart Card or making the ID Smart Card have access to the User's banking accounts, which is what some projects are trying to do in order to minimise the number of cards that Users carry in their purses. This will make the User more vulnerable to attacks and the consequences will be more harmful.

Now, the point behind specifically listing the contents of each type of smart card is to reveal the fact in case the User's purse gets lost or stolen, taking into account that in our days the purse probably holds at least two types of the previously listed smart cards. Thus, when an attacker gets hold of the banking card and any other smart card in the purse, then breaching the User's banking system is not a problem. The attacker can get hold of the User's identification details including date of birth and address, in addition to the User's account details. Then, the attacker will easily identify himself to the system and enjoys spending money or doing other things after successfully stealing the User's identity.

On the other hand, if getting access to the smart card contents is very much complicated and requires the User to be present for banking and identification transactions to take place, then the smart card will be a better option. So, there must be great emphasis on making the User and Smart Card work together and

not only depending on the smart card. Also, the less details the smart card holds, the less the risk is.

4.2.3 The Smart Card System Objects and Operations

Previously, the main elements of any smart card system and the operations that each element is responsible of in the system were mentioned. This section will present some UML sequence diagrams that will demonstrate the smart card system objects along with their associated operations and transactions in more details but within the system transaction level. It is quite essential to know exactly what happens while using a smart card. Thus, the following sequence diagrams will show the transactions that take place in the currently implemented smart card systems [141].

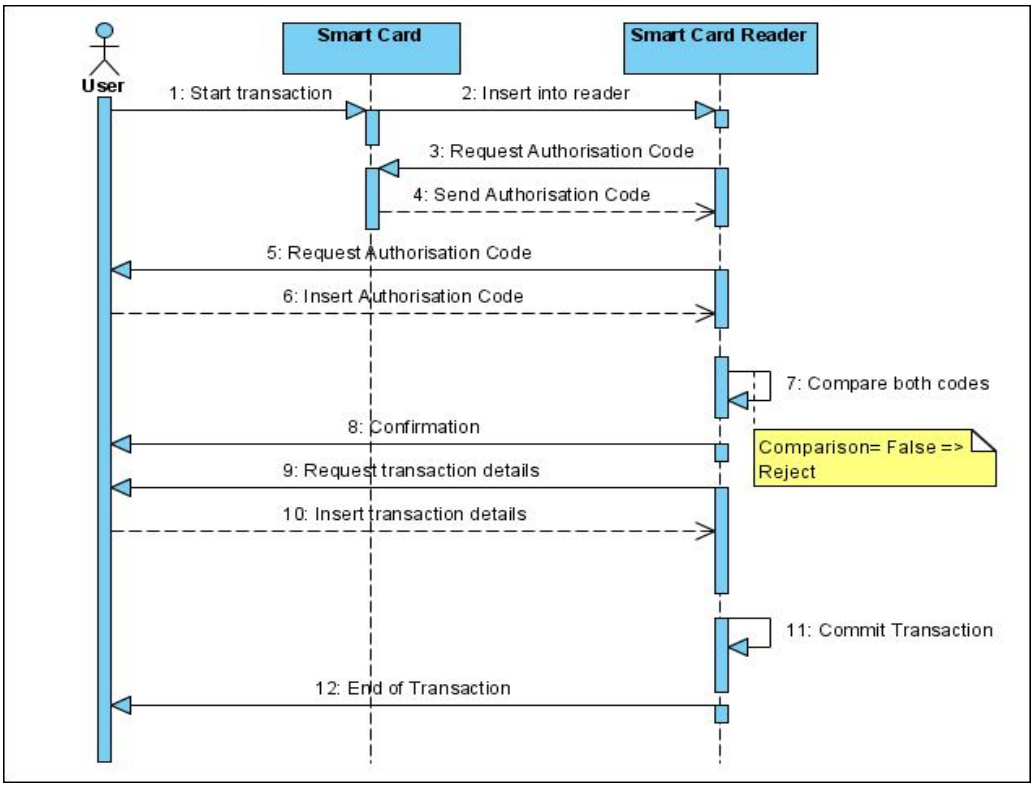

Figure (14): Sequence Diagram- Using a Smart Card and a Smart Card Reader

In any smart card system, the User will only interact with the Smart Card and the Smart Card Reader. Figure (14) demonstrates the transactions that take place when a User wants to use the Smart Card to commit an operation regardless of what type of Smart Card is used, the transactions details are derived from the daily actions that occur whenever we use a smart card in any point of sale or ATM.

Transactions (1 and 2): the User inserts the Smart Card into the reader and then the verification process starts.

Transactions (3-6): the Reader will request a verification code to be inserted by the user depending on what type of security mechanism is applied to the system. Thus, the code could be a PIN/Password, Biometric, or a combination of multiple mechanisms, etc.

Transactions (7 and 8): the Reader then starts a matching process between the inserted code and the code stored in the Smart Card. If the matching process was true, then the Reader will confirm that the individual is who the individual claims to be and proceed with the transaction; otherwise, the Reader will reject the User and ends the transaction.

Transactions (9-12): after getting the confirmation from the Reader to proceed with the transaction requested by the User, the User inserts the transaction details through the Reader. Finally, the Reader commits the transaction and informs the User when the transaction is over.

If the smart card system is using the PIN/Password as a security mechanism along with the Smart Card, then the Registration System will generate a random PIN/Password during the User enrolment process and will send the code to the

User. Or the User can register the PIN/Password during the enrolment process and this will be saved in the system. However, it is important to mention the weaknesses of using such a mechanism; the truth is PINs and Passwords represent significant risks because the User is in total control of the code. The User can share the code with others, write the code down on the card or somewhere close to it, use simple codes that can be guessed, in addition to the high probability of using the same code across multiple systems. Unfortunately, most of the currently implemented smart card systems rely heavily on this security mechanism, which results in high system breaches and identity theft. The coming corrections to the smart card systems are focusing on using the Biometrics technology as a much safer security mechanism in comparison with the PIN/Password.

Smart Card Systems with Biometrics as a Security Mechanism

Figure (15) is a sequence diagram that demonstrates the registration process of the Biometrics mechanism along with the verification process that is derived from [66]. The registration process and the smart card issue process are similar to [66], however, there are differences in the verification process. In [66], the authors came up with a new signature system model that has no matching process. The private keys in their proposed model were generated from fingerprint minutiae; they also added a check bit string and a rememberable key to the signing process. Their proposed new signature system is just a model and needs more work to become a practical system. Therefore, the new signature system model from [66] has been excluded from the models in this study.

The Issuing Authority of the Smart Card must implement a trusted smart card system; therefore, focusing on the design of the system is one of the most important issues to be concerned of. The design of a secure smart card system must have a secure enrolment process and a secure verification and authentication process. The enrolment process is part of the Registration System that is responsible of collecting the User's information, ensuring that the User is entitled of the credentials and privileges granted, and issuing the Smart Card. The first number of transactions in figure (15) shows the registration part of the system.

Transactions (1 and 2): the User applies for the Smart Card and therefore provides the required information and details to the Registration System. The Registration System must make sure that the information provided is of high quality and accuracy, the User must prove his/her identity to the system by using various methods.

Some of these methods are less secure like for example applying by filling a registration form and sending it by mail or e-mail, on the other hand, a more secure method is in-person identification, which is the most common method and is the most accurate. The Registration System must also ensure that the User has not enrolled in the system before as someone else; therefore, the enrollers must be well trained and aware of such cases.

Transactions (3 and 4): after making sure everything is fine and all the data are accurate, the Registration System saves the User information in the Smart Card and requests the User biometric to establish the security process.

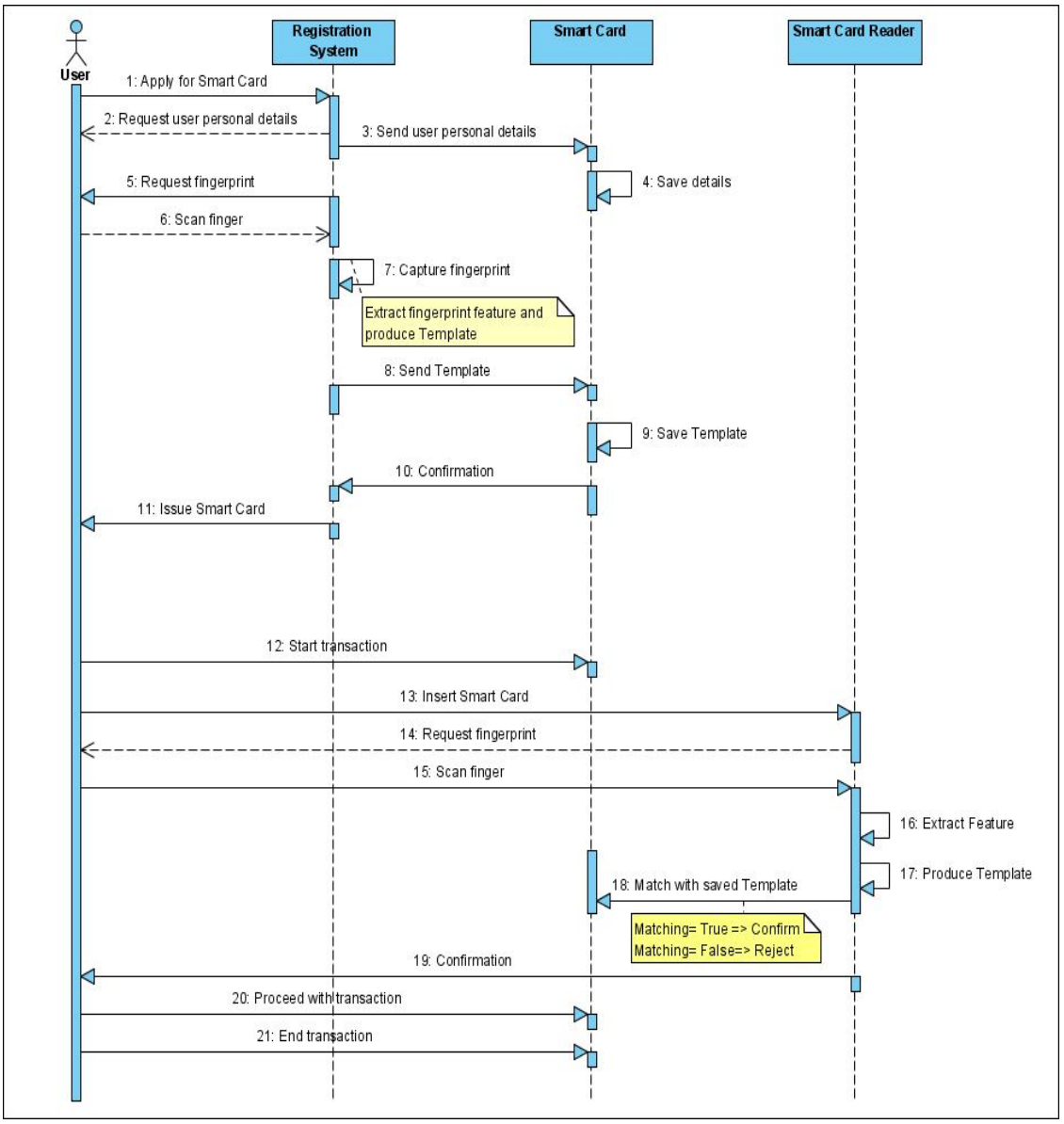

Figure (15): Sequence Diagram- Biometrics Enrollment and Verification Processes in a Smart Card System

Transactions (5-7): the User provides the required biometric evidence to the Registration System, which is the fingerprint in this case, the evidence captured must be of a very high quality and accuracy, otherwise, the system performance and accuracy will be decreased and will perhaps produce false results.

Transactions (8 and 9): the Registration System issues a template and saves a copy of it in the User's Smart Card for future use during the verification process.

Transactions (10 and 11): the Smart Card confirms that the details are saved, so the Registration System issues the Smart Card for the User.

The second part shows the verification process of the smart card system using biometrics as a security mechanism. At this point, the Registration System is not any more involved.

Transactions (12 and 13): The User starts the transaction and inserts the Smart Card into the Smart Card Reader.

Transactions (14-17): the Reader will request the security code that is the biometric evidence in this case, the User then scans his/her finger and the fingerprint is extracted and transformed into a template using the related algorithms.

Transactions (18-21): the Smart Card then compares the provided template to the one saved in the system and produces the matching result. If the result was true, then the Reader confirms the User identity and proceeds with the User transactions, otherwise, reject the User and ends the transactions.

An important issue to point out is that currently the systems have not yet used this criterion of fingerprint live extraction method. The required algorithms for this method have not yet been developed and used successfully. Therefore, the systems use the template stored in the Smart Card and compare it to the template stored in the database of the system.

Smart Card Systems with Biometrics and PKI as Security Mechanisms

The following figures demonstrate the use of Biometrics mechanism along with the PKI security method, which is derived from [66] and [142]. Again, as

mentioned in the previous section, the new signature system model that was proposed in [66] has been excluded. In [142], the authors examined five scenarios with three different strategies for integrating fingerprints into a smart card system, the outcome showed that the scenario where the match operation is performed on the smart card with the fingerprint sensor being built into the smart card reader is the most beneficial in the smart card-card reader model. Therefore, the models of this study are derived from the scenario that came up with the best results in [142], and added the PKI transactions to it.

The biometrics mechanism is responsible of identifying and verifying the User, on the other side, the PKI is handling the identification and verification of the devices that are used in the system. Hence, two diagrams were created, the first diagram demonstrates the registration phase of the system and the second diagram demonstrates the process of using the smart card to commit a transaction in any smart card system that employs Biometrics and PKI. Figure (16) focuses on the Registration System that consists of the enrolment process.

Transactions (1-4): at the beginning, the User has to enrol in the smart card system by applying for a Smart Card, providing personal details, proving to the system that the User is who the User claims to be by showing the relevant proof, and providing the biometric evidence depending on the biometric evidence type employed in the smart card system, which is in this case, the fingerprint.

Transactions (5-9): the Registration System extracts the biometric feature and transforms it into a template. The template is saved in the system and the Smart Card for future use in the verification process.

Transactions (10): after saving the template, the smart card issue system requests a secret key or also called private key from the Certificate Authority (CA), which is the authority responsible of generating digital certificates and a pair of private and public keys to the Users.

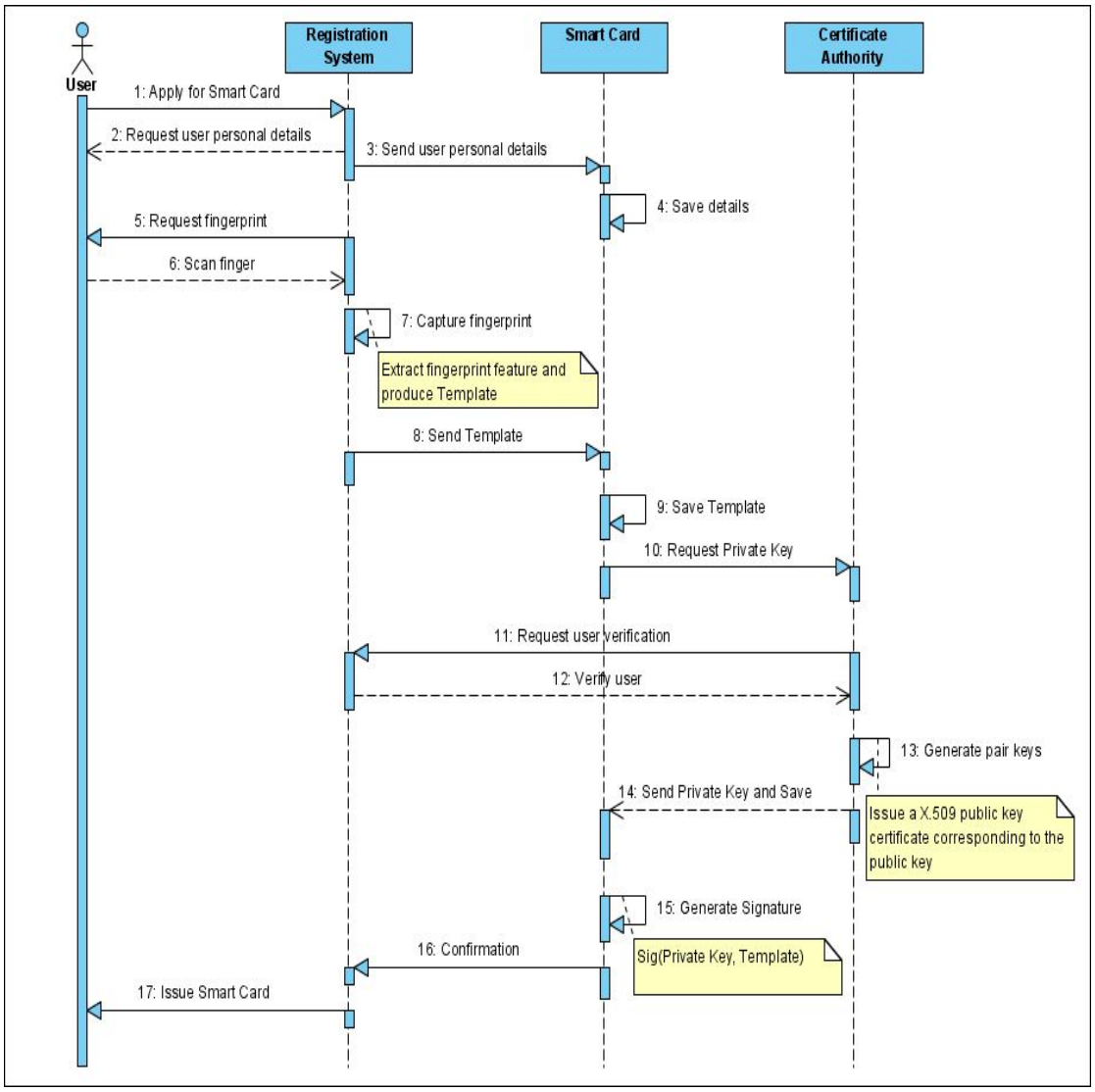

Figure (16): Sequence Diagram- Registration Phase in Biometrics and PKI Smart Card System.

Transactions (11-13): the CA first makes sure that the User is who the User claims to be by requesting User verification from the smart card system, if the verification was successful, then the CA issues a pair of private and public keys

to the User and generates a digital certificate in correspondence with the public key.

Transactions (14): the CA then stores the User's public key in its databases and sends the private key to the smart card system.

Transactions (15): the Smart Card issue system then generates a digital signature that contains the User's private key and the biometric template.

Transactions (16-17): finally, the smart card issue system sends a confirmation to the Registration System and the Smart Card then is going to be issued successfully to the User.

Hence, in order for the User to successfully use the Smart Card, the matching process of the biometric evidence must take place along with the correct matching of the private and public keys.

Figure (17) will show the transactions that take place when the User uses the Smart Card in a security environment that combines both Biometrics and PKI security methods.

Transactions (1-3): the User first scans the finger through the Smart Card Reader scanner; the Reader will extract the User's biometric feature and produce a template.

Transactions (4 and 5): the matching process will then take place and the result will decide whether the User has the permission to access the system and use the Smart Card or not. If the matching result was true, then the Smart Card will release the User's private key and the verification process will then be successful.

Transactions (6 and 7): the User starts to send a message to the Receiver; the message is going to be digitally signed with the User's private key first.

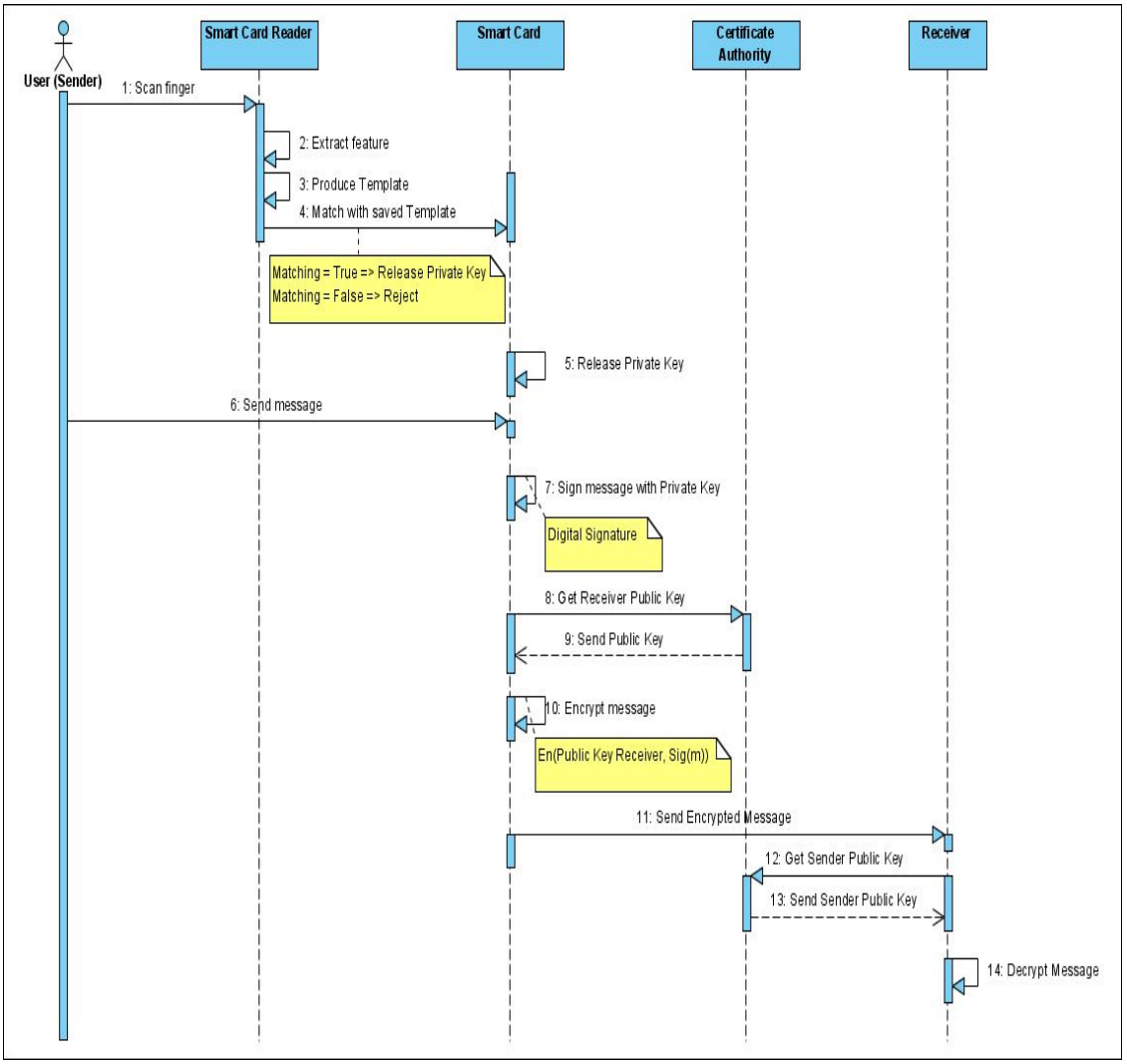

Figure (17): Sequence Diagram- Verification Phase in Biometrics and PKI Smart Card System.

Transactions (8-11): then the system will request the Receivers public key from the CA in order to encrypt the message. The CA will send the digital certificate and the message will be encrypted using both the User's private key and the Receiver's pubic key, therefore, the digital envelope is now ready to be sent securely to the Receiver.

Transactions (12-14): finally, the Receiver will send a request to the CA to get the Sender's public key to be able to decrypt the message. Again, using both the Sender's public key and the Receiver's private key the Receiver will be able to open the message successfully.

Using these security methods will achieve the security goals, which are confidentiality, integrity, authentication, and non-repudiation. However, each mechanism has its pros and cons, and the fingerprint has its disadvantages. The question that arises in this situation is: How can we know that the biometric provided is not subject to misuse? If the User was clever and powerful enough to fool the system and use a false fingerprint, then the system will be breached and an intruder will have access to the real User's credentials and privileges. In addition, the PKI method has its disadvantages as well, in case one of the disadvantages take place during the transaction the Sender and the Receiver will both suffer from security loss.

4.2.4 The Smart Card System Proposed Designs

Putting in mind that each security mechanism can be breached in a way or another, some proposed smart card systems are generated to overcome some of the disadvantages of those mechanisms. Combining number of technologies to achieve a better secured system is a great idea, as mentioned as ideas and recommendations in [26] and [143] . The combination will improve the system security and better protect the information that flows within the system components.

Smart Card Systems with PIN, Biometrics, and PKI as Security Mechanisms

The first proposed system design combines three security mechanisms in addition to the Smart Card that is based on "what the user has". The mechanisms are: PIN, Biometrics, and PKI, The first two mechanisms are responsible of User identification and verification, a PIN mechanism is based on "what the user knows", and the biometrics is based on "who the user is". Furthermore, the PKI mechanism is the key management method that is responsible of verifying the devices in the system.

The design is divided into two sequence diagrams, the first diagram demonstrates the Registration System and the other diagram demonstrates the Verification process along with the transactions related to sending the messages between the sender and the receiver.

Figure (18) shows the enrolment process that is the main part of the Registration System. Similar to the previously described system designs that were derived from [66]; however, it goes beyond what was previously published by adding two authentication mechanisms during the Registration System.

Transaction (1-9): the User provides the required information along with the biometric evidence. The system then saves the User details in the Smart Card and captures the fingerprint, which is the biometric method used in the proposed design, and produces a template that is stored in the system and the Smart Card.

Transaction (10-12): the Registration System requests a PIN from the User to be used in future verification processes along with the biometric evidence. In some cases, the PIN can be generated by the Registration system randomly and sent to

the User, after that the User has the ability to change the PIN into a code that the User can memorise. The PIN is going to be stored in the Smart Card to be able to achieve future verification.

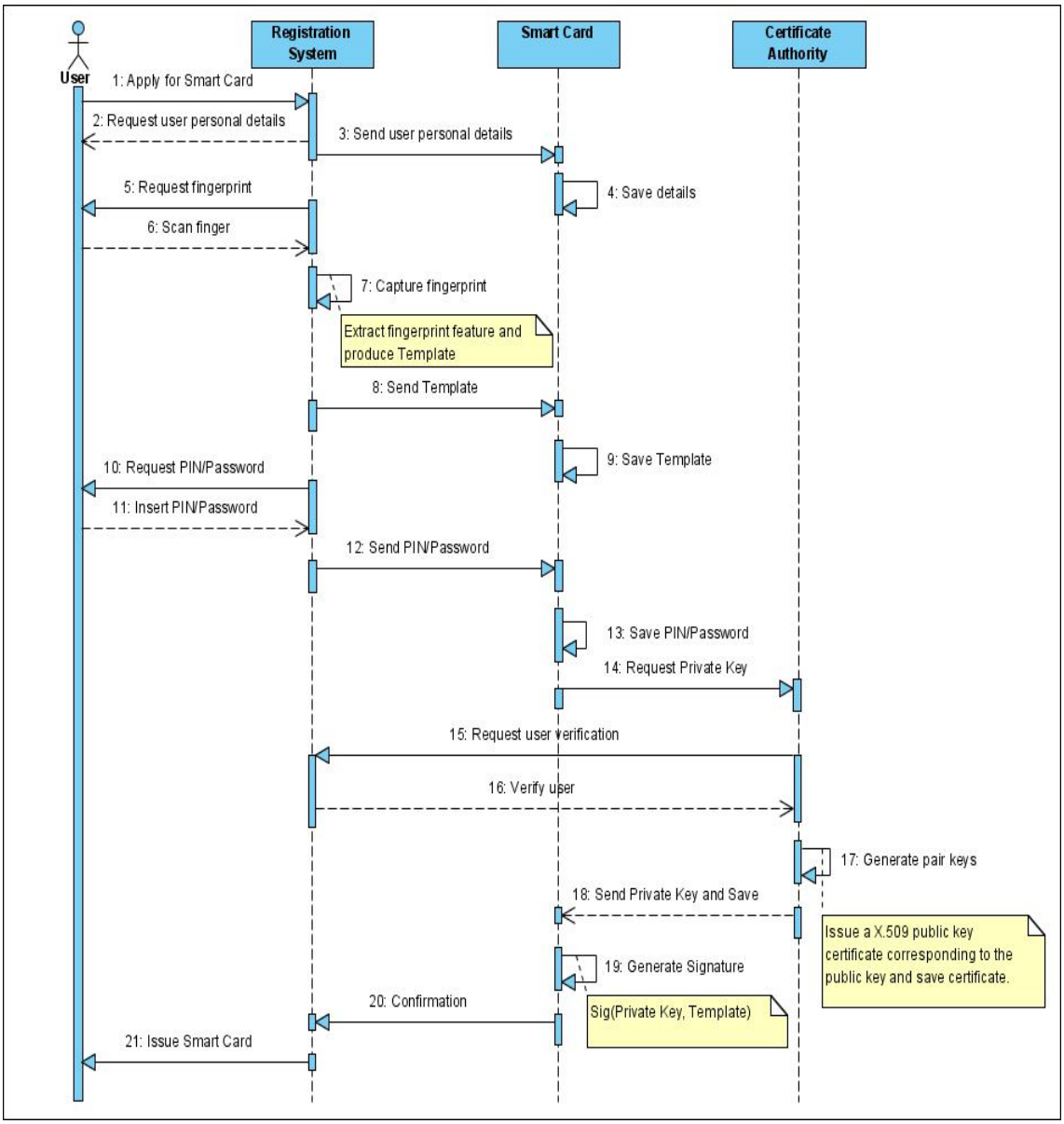

Figure (18): Sequence Diagram- Registration Phase in PIN, Biometrics (Fingerprint), and PKI Smart Card

Transaction (13-18): the smart card issue system requests a private key from the CA to be able to generate a digital signature. The CA on the other hand requests

User verification from the Registration System, generates a pair of keys to the User, the CA also issues a digital certificate corresponding to the public key, and after all sends the private key to be stored in the Smart Card.

Transaction (19-21): the Smart Card generates a digital signature that combines the private key and the biometric template of the User. Then the Smart Card sends a confirmation to the Registration system, therefore the new Smart Card is issued and sent to the User.

Figure (19) shows the transactions that take place when the User uses the Smart Card in a security environment that combines PIN, Biometrics, and PKI security methods.

Transaction (1-4): the User inserts the PIN first; next the Smart Card Reader will extract the saved PIN from the Smart Card and start the comparison process. If the matching was successful the Smart Card Reader will ask for another proof, which is the User's fingerprint, otherwise, the transaction will be aborted after allowing the User generally three attempts to enter the PIN.

Transaction (5-7): the User then scans the finger through the Smart Card Reader scanner; the Reader will extract the User's biometric feature and produce a template.

Transaction (8 and 9): the matching process will then take place and the result will decide whether the User has the permission to access the system and use the Smart Card or not. If the matching result was true, then the verification process will be successful. This will make the Smart Card chip unlock and release the User's private key. The Smart Card is now ready to use the released private key to digitally sign the message that is going to be sent by the User.

Transaction (10 and 11): the User starts to send a message to the Receiver; the message is going to be digitally signed with the User's private key through the Smart Card.

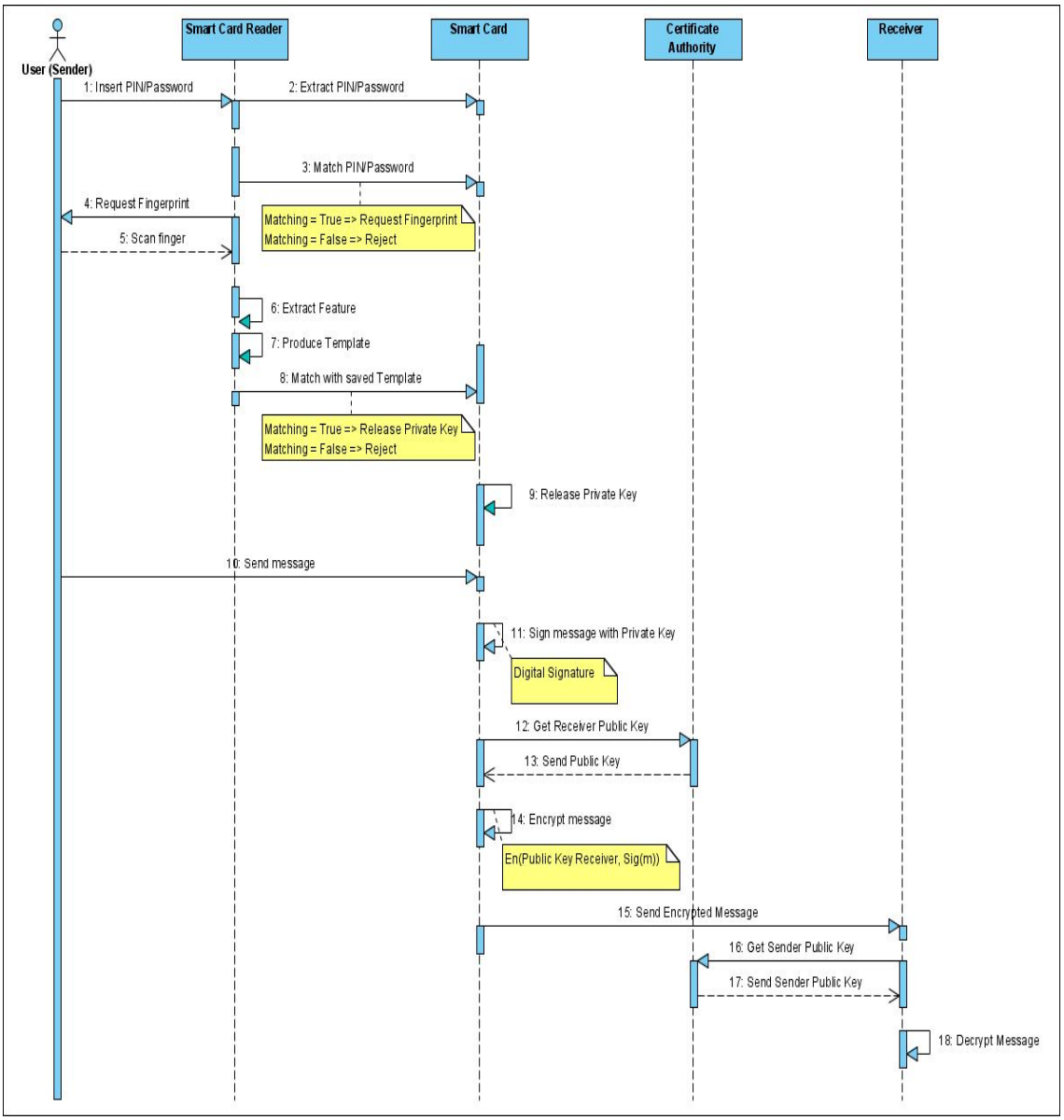

Figure (19): Sequence Diagram- Verification Processes in PIN, Biometrics (Fingerprint), and PKI Smart Card System.

Transaction (12-15): then the system will request the Receivers public key from the CA in order to encrypt the message. The CA will send the digital certificate

and the message will be encrypted using both the User's private key and the Receiver's public key, therefore, the digital envelope is now ready to be sent securely to the Receiver.

Transaction (16-18): Finally, the Receiver will send a request to the CA to get the Sender's public key to be able to decrypt the message. Again, using both the Sender's public key and the Receiver's private key the Receiver will be able to decrypt the message successfully.

Smart Card Systems with Two Biometrics and PKI as Security Mechanisms

Another suggestion is to use two Biometric methods rather than a PIN and a Biometric method for user authentication, which is a further enhancement of what have been previously published. It is more significant to use one physical biometrics method and another behavioural biometrics method, the reason behind using two different biometric methods is to make sure the user is who he/she claims to be. If the attacker was successful in fooling the authentication scheme with a fake fingerprint, the attacker will have to succeed again in the next authentication step that is another biometric evidence to submit, which make it harder for an attacker have successful attempts on both biometric methods. Attacking Biometrics is possible but is much harder than attacking a PIN, therefore, there is a better chance that the probabilities of successful attacks will decrease.

Figure (20) is a sequence diagram that shows the transactions that take place in a smart card system which employs two Biometric methods: fingerprint as a physical biometric method and signature as a behavioural biometric method. The

registration system in this proposed system is quite similar to the previously described Biometrics Registration System; also, this system employs PKI as the cryptographic key management scheme, which has a third party that produces digital certificates to the system users allowing them to store their private keys in their smart cards and exchange public keys throughout the network.

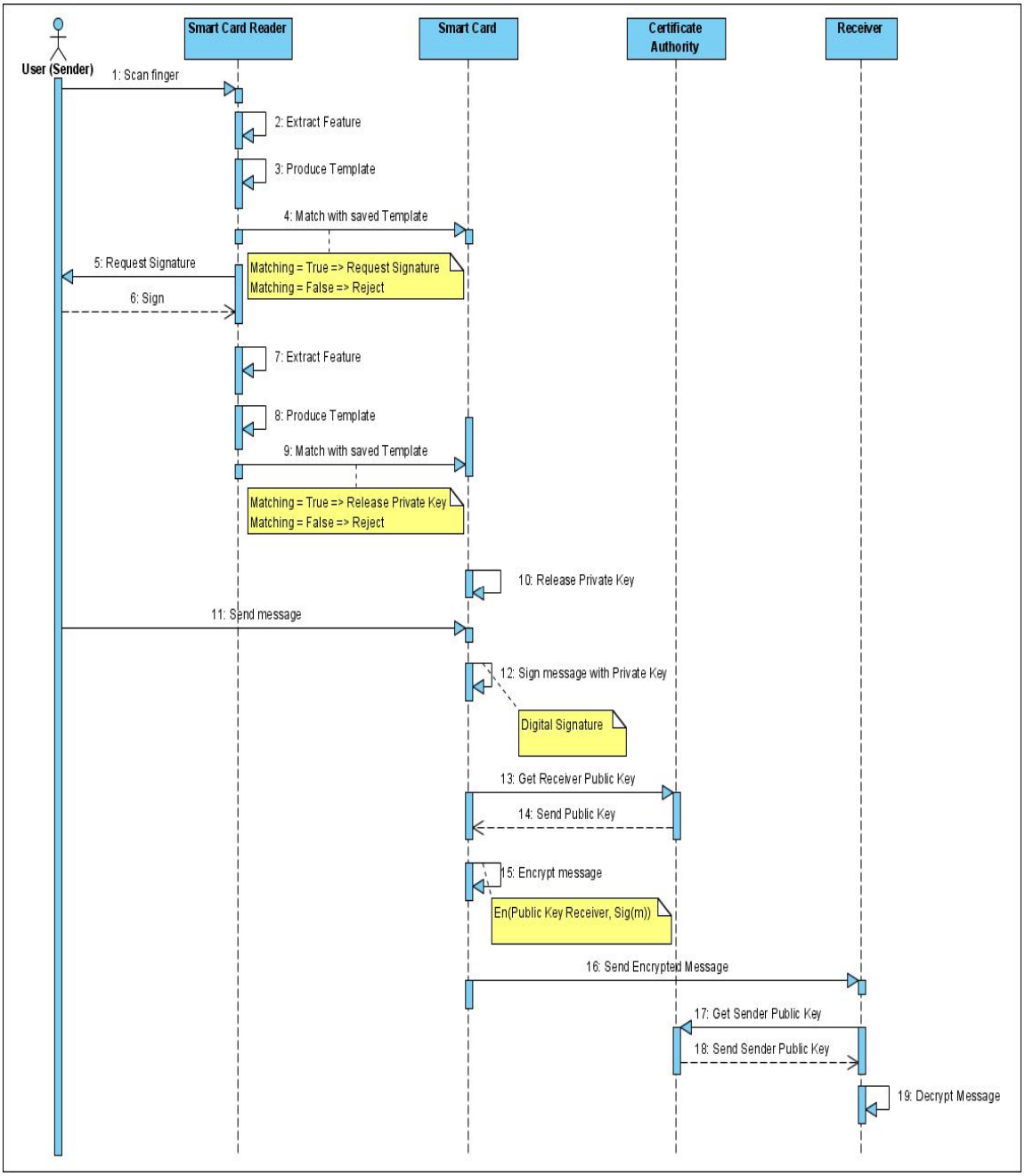

Figure (20): Sequence Diagram- Verification Processes using two Biometric methods (Fingerprint and Signature), and PKI.

Transaction (1-5): the User submits the fingerprint first, and then the matching process will match the live template produced with the stored template. If the attempt was successful, then the system will request the User's signature. Otherwise, another attempt will be given to the user to be able to submit the correct fingerprint.

Transaction (6-9): the User is going to sign using the digital screen on the Reader. Then the Reader will extract the features, generate a template out of the live signature, and match it with the template saved in the smart card. The result of the matching process will determine whether the user is the legitimate user or not. Each system has the flexibility to allow number of attempts, usually the systems allow the users three times to submit the correct evidence.

Transaction (10-19): these transactions are similar to the previously explained transactions in figure (19). The Smart Card will release the private key, digitally sign the message, encrypt the message using the Receiver's public key, and send the message to the Receiver. Finally, the Receiver will decrypt the message using the Sender's public key.

In conclusion, it is much better to use combined methods of authentication to be able to better secure the system, there are number of options when it comes to combining authentication methods. According to the security requirements, type of information, amount of information stored and transmitted throughout the network, and some other factors depending on each type of smart card system and the services it provides, the system administrators will have to choose the methods that better serve their systems and ensure good security levels.

4.3 Attempt to Test Against Attacks by Using UMLsec

Three types of UML diagrams have been used, which are behaviour diagrams (Use Case diagram), structure diagrams (Class diagram), and interaction diagrams (Sequential diagram). The UML diagrams are used to express the smart card system protocol and processes, and present the transactions that take place while messages are exchanged during the registration and verification processes, in addition to knowing where are the areas that could be vulnerable to attacks, it is quite essential to test the model against possible attacks. UMLsec was used to test attacks against the model, stereotypes like <<*secrecy*>> and <<*secure information flow*>> along with their tags and constraints were applied. An adversary type in UMLsec can have a function called Threat that allows the adversary to commit delete, read, and insert as attacks. By writing these notations down, the model is still static and not executable.

As a result, UMLsec is a well developed extension of UML; however, it did not automate the model. The reason is that UMLsec is a specification language that has the ability of expressing the system protocols and transactions but not automating them. Therefore, in this piece of work, we are trying to provide a simulation tool, which is the next step after modelling the system using specification languages that produce diagrams and notations. For that reason, SystemC with TLM extension is going to be used to be able to transform the static model into an executable model.

4.4 Concluding Remarks

The UML diagrams produced in the chapter gives the designer a detailed view of the smart card system components and functions. The diagrams illustrate the system objects and assign the transactions to be carried out by each object, in addition to demonstrating the system processes that take place from the beginning until the end. UML as a modelling language has a strong visual component that allows the construction of models at varying levels of abstraction, it also allows the designer to propose solutions and demonstrate them at different levels of detail.

The diagrams can be static or dynamic, in this chapter both types are used to better demonstrate the smart card system components and their related transactions. The static diagrams used are the use case diagram and the class diagram, these diagrams offer a structural view of the smart card system, examples are figure (12) and figure (13). On the other hand, the sequence diagram used is a dynamic type of diagram that shows the behaviours and interactions of the smart card system components, examples are figures (14-20).

However, to be able to take this model to a further advanced step, which is automation, the UML and its related extensions do not have the ability to support the designer's needs. Therefore, the next chapter is about using other languages that are capable of transferring the static diagrams produced in this chapter into an automated model that allows transaction execution.

Chapter 5

Smart Card System Simulation Using SystemC and Transaction Level Modelling (TLM)

Modelling and producing a simulation tool that allows the designer to run tests on the proposed smart card systems is the aim of this chapter. SystemC along with its extension TLM are used to build the smart card system simulation tool, which is an executable model that can run different number of tests and therefore gives the designer the opportunity to examine the robustness of the smart card system security.

5.1 Simulating the Smart Card System

In essence, it is meaningful and quite significant to demonstrate the diagrams and produce a simulation tool based on it to be able to know that the model is correct. Otherwise, without simulation there is no chance of declaring that the model is correct and is running in an effective and efficient manner.

The previous modelling languages do not provide an automatic transition from design to code implementation; the designer would like to have an executable model that allows a better testing of the designed model and therefore links the gap between the design phase and the code implementation phase. Therefore, in this study, the executable model is produced using SystemC with the TLM extension.

SystemC has become a popular choice for designers of both System-On-Chip (SOC) and embedded processors, the reasons behind the popularity of the language is its adaptability at cycle, facilitating the development of transaction level models (TLM), and ability to model concurrent processes [144], [145]. The following is a description of SystemC language along with TLM, which are both used to test the proposed solutions to be able to enhance the smart card security system.

5.1.1 SystemC Overview

SystemC consists of a class library and a simulation kernel, the language is supported by Open SystemC Initiative (OSCI). SystemC was defined by the OSCI [146] as:

> SystemC is a single, unified design and verification language that expresses architectural and other system-level attributes in the form of open-source C++ classes. It enables design and verification at the system level, independent of any detailed hardware and software implementation, as well as enabling co-verification with RTL design [146].

The designer creates the SystemC models at different levels like system level, behavioural level, or register transfer level (RTL) using C/C++ augmented by the SystemC class library [147]. The SystemC library uses many types of hardware specific objects like concurrent and hierarchical modules, ports, channels, processes, and clocks. In addition, it contains a light weight kernel that schedules the processes [147].

SystemC is a design language that has developed to support the need for a language that improves the overall productivity for designers in the electronic systems field [148]. The common approach to the development of (SoC) requires a

software model using some high level language such as C and C++, on the other hand, a hardware model using some hardware description languages such as VHDL and Verilog is also required [149].

However, it is quite a hard task to communicate with the software using the previous hardware languages and vice versa, so the software engineer must interact with the established hardware model in ways such as remote procedure calls or socket communication [149].

SystemC increases productivity by giving the engineers and designers the opportunity to design both hardware and software components at the same time [148], it supports the development of complex systems by designing and verifying hardware system components at a high level of abstraction [150], [145]. By providing a higher level of abstraction, a greater understanding of the system components interactions and complexity in the early stages of design will be possible, in addition to enabling considerably faster, more productive architectural trade-off analysis, design, and redesign. SystemC was used by [151] to produce a methodology to simulate security attacks on smart cards with fault injection, it was also used by [145] to create an environment for design verification of smart cards using security attack simulation, their work specifically focused on testing the robustness of systems against optical fault induction attacks. SystemC represented designs on high abstraction levels with a shorter simulation time, which gives the advantage of redesigning the system to fulfil certain security demands. However, the executable model with attacks simulation in this study is different from the work in [151] and [145] because the simulation includes more than one type of attack, plus the testing of the system

robustness is done on the transaction level using the transaction level modeling extension that is going to be explained in the coming section of this chapter.

5.1.2 SystemC Components

The major hardware oriented features implemented within SystemC are: Module Hierarchy, concurrency model, time model, communications management between concurrent units of execution, and hardware data types [148]. As mentioned previously, the SystemC library provides concurrent and hierarchical modules, ports, channels, processes, and clocks. Large designs are always broken down hierarchically to be able to manage complexity; structural decomposition of the simulated model in SystemC is specified with modules. The module is the smallest component with state, behaviour, and structure for hierarchical connectivity, the concept known as SC_MODULE is used to represent the module [148]. Within the module, a variety of elements make up the body, however, the constructor is one of the main elements required in every module. It performs number of tasks such as initializing/allocating sub-designs, connecting sub-designs, registering processes with the SystemC kernel, providing static sensitivity, and miscellaneous user-defined setup [148]. The constructor concept in SystemC is known as SC_CTOR, or sometimes SC_HAS_PROCESS that is an alternative approach to creating constructors by using a C-preprocessor (cpp) macro [152].

Modules are considered to be the building blocks of SystemC; the interaction between modules is designed using channels, interfaces, and ports. A channel is the base communications mean that is in charge of propagating values from one point of the design to the other. A channel is more than a simple signal in

SystemC, channels represent complex communications schemes like bus channels, at the same time, they may represent very simple communications such as a wire or a FIFO (first-in-first-out queue) [150].

A SystemC interface is an abstract class that provides pure virtual declarations of methods referenced by channels and ports [148], furthermore, ports rely on interfaces to communicate with channels. A port is a pointer to a channel outside the module, it allows access of channels across module boundaries [152].

The functionality of SystemC is described in processes, the process is a basic unit of execution in the system, from the start of the simulation until the end all executing code is initiated from one or more processes, in addition, SystemC processes represent concurrent behaviour [148], [147]. There are two basic types of processes, methods known as SC_METHOD and threads known as SC_THREAD. Method is a process that behaves like a function call, it is in some ways more simple than a thread process, however, its simplicity makes it more difficult to use for some complicated modelling styles [147]. Methods cannot be suspended internally, instead, they can run completely and return, the simulation engine calls the methods repeatedly based on the type of sensitivity, whether dynamic or static. This characteristic makes the method more efficient than the thread process. On the other hand, a thread process is associated with its own thread of execution, this type of processes start one only by the simulator, once the thread starts executing it is in complete control of the simulation until it chooses to return the control to the simulator. Hence, the thread process is used to model sequential behaviour [147]. SystemC has two

ways to pass the control to the simulator again, one way is to exit by (return), in this case the thread is totally stopped, the other way is by having a (wait), therefore, every thread contains an infinite loop usually has at least one wait function. Therefore, SystemC enters the waiting state whenever it encounters a wait or a return.

It is important to mention events in SystemC, an event is considered to be a critical element in an event driven simulator similar to the SystemC simulation kernel [148]. It is known as sc_event, it has no value and no duration, it is mainly the occurrence of an sc_event using the notify keyword that happens at a single point in time.

The SystemC simulation kernel follows the evaluate-update concept, where multiple evaluate-update phases can take place at the same simulation time is supported [147]. The phases are initialisation, where the system is initialised by executing all the processes. Second, the evaluation phase, which is about executing the process that is ready to run, it is repeating until all ready processes are executed including events. Last, the update phase that is executing any update calls made during the evaluation phase [147]. This is mainly the basic phases of the SystemC simulation kernel along with the basic components that are included in models produced and designed by SystemC.

5.1.3 Overview of Transaction Level Modelling (TLM)

In TLM, communication among computation components is modeled by channels and transaction requests, which are implemented by calling interface functions of these channel models [153]. The initiator port and the target port are distinguished in TLM [154], an initiator is a module that creates new

transactions and passes them on by calling a method of one of the core interfaces [155], and the target is another module that receives the sent transactions from the initiator. A system component can be an initiator, a target, or an interconnect. The interconnect module accesses a transaction but does not act as an initiator or a target for that transaction, for example routers can be interconnect modules in a system [155], [156]. Another important element in TLM is the generic payload, which is defined by [155] as a class for transaction objects passed through the core interfaces of the model, it is closely related to the base protocol that ensures interoperability when using the generic payload. The generic payload is aiming at modeling memory-mapped buses, which includes some of the memory-mapped bus protocols attributes like command, address, data, byte enables, single word transfers, streaming, response status, etc [155], [156].

TLM enables high speed simulation time in addition to exploring and validating implementation alternatives at a high level of abstraction [153]. TLM have been successfully used in the design of systems by some designers and developers; it was used by [157] to ease the development of embedded software, and [158] applied TLM with protocol details and used it to integrate system components at the transaction level. Therefore, TLM has number of benefits that allows the designer to design the communication of the system components in a high level of abstraction with less simulation time, in addition to the ability of redesigning the transactions in an easier and more convenient manner.

5.1.4 Producing the Smart Card System Simulation Tool

The main idea in this section is to produce a simulation tool, which has the ability to transform the static UML diagrams demonstrated earlier into a program that executes the transactions in an automated manner.

5.1.4.1 The Structure and Processes of the Smart Card Simulation Tool

The executable model produced in our work shows the sequence of transactions that occur in the smart card system while the smart card is used; they correspond to the transactions in the figure (19), where the smart card system uses the PIN and Biometrics for user identification, and PKI as a key management security method. Figure (19) is the diagram chosen among others to be transformed into code because it includes all the smart card system components, two different authentication methods, a key management method, and it demonstrated all the transactions that occur in the processes of the smart card system.

Hence, in the executable module, the smart card system objects and their related transactions, the lifelines in the UML diagram, are represented as objects - modules in SystemC, and the arrows are represented as TLM transactions. The modules have two types of sockets, an initiator socket that is responsible of sending the transactions and a target socket that is responsible of receiving the transactions; both sockets are defined in the module structure. Figure (21) shows an example of one of the modules, which is the Sender module.

The Sender module communicates with the Smart Card module and the Smart Card Reader module. An initiator socket from the Sender to the Smart

Card is created, along with another initiator socket to the Smart Card Reader module, to allow the Sender to send transactions to both modules. The initiator is responsible of calling the transport function to send the payload to the target socket. On the other hand, a target socket is created and then registered in the constructor; the target socket receives the payload from the transfer function for processing and response.

```
SC_MODULE(sender)
{
     // smartcard reader interface
     simple_initiator_socket<sender> iS_to_smartcard;

     // smartcard reader interface
     simple_initiator_socket<sender> iS_to_smartcard_reader;
     simple_target_socket<sender> tS_from_smartcard_reader;

      SC_CTOR(sender) {
            // target socket registration
            tS_from_smartcard_reader.register_b_transport(this,
&sender::b_transport);
            // main thread
            SC_THREAD(state_machine);
            // state machine initial state
            state = START;
      }
```

Figure (21): The Sender Module Structure of the Smart Card System

In this case, the Sender receives transactions from the Smart Card Reader module and processes them.

The next step is creating the threads that correspond to the processes taking place in each module, creating the payloads that are transferred from a module to the other, creating functions, and setting events and variables. In the smart card executable model, the authentication methods used are PIN and Biometrics. The user, modelled as part of the Sender module, enters the PIN first. If the PIN is correct, the Sender enters the fingerprint. The number of attempts allowed for the Sender is programmable and flexible to change; the system administrators

and decision makers have the authority to decide the number of attempts allowed by simply changing the rule of number of attempts.

For example, in our case the Sender has three attempts to enter the correct PIN and other three attempts to enter the correct fingerprint. The executable model counts the number of attempts, and compares the inserted PIN and fingerprint with the saved PIN and fingerprint template in the smart card. Also, there is a time limit for inserting the PIN and fingerprint, the Sender has ten seconds to enter the data, otherwise a timeout message will appear and one attempt will be counted as incorrect. If the number of incorrect attempts exceeded the limit, which is in this case three times, the system blocks the smart card and saves the smart card ID in the banned smart card list. Errors in entering the correct PIN vary; it could be wrong digits, taking long time to insert the correct PIN, or an attacker trying to insert the PIN randomly, etc. So the steps that take place during the authentication process are:

Get PIN
If PIN inserted = Saved PIN
If Time is < 10 seconds
Then print “Correct”
Request fingerprint
Else If re-enter PIN
If number of attempts < 3 times
Go to Get PIN
Else block the smart card and print “max pin attempts reached card banned”

Figure (22) shows a sample of the SystemC TLM code lines of the previous pseudo code:

```
void generate_transaction(string &pin_, sc_time &dt_) {
            scv_smart_ptr<int> correct_entry_ptr;
            correct_entry_ptr->keep_only(1, 100);
            correct_entry_ptr->next();
            if ( *correct_entry_ptr > PIN_FAILURE_RATE) {
                  pin_ = "correct";
            } else {
                  pin_ = "incorrect";
            }
            scv_smart_ptr<int> time_value_ptr;
            time_value_ptr->keep_only(1, MAX_ENTRY_TIME);
            time_value_ptr->next();
            dt_ = ( (*time_value_ptr) * sc_time(1, SC_SEC));
            }
```

Figure (22): The PIN Entry Part of the Simulation Tool

The same steps take place when entering the fingerprint, the successful attempts of PIN and fingerprint will confirm that the Sender is the legitimate user. Therefore, when the Sender passes the authentication step, the smart card releases the private key, and the transactions related to signing the message with the private and public keys, in addition to sending the digitally signed message to the Receiver occur.

In reality, the User enters the PIN and scans the fingerprint through an input device like a key pad, biometric scanner, or a touch pad. However, our executable model can randomise the PIN and fingerprint entries, and also randomise the correct and incorrect time. A simple pseudo-random number generator is used to be able to randomise the PIN and fingerprint entries along with randomising the correct and incorrect time in seconds. The simple random number generator is fast and provides better randomness properties like adjusting the ratios, changing the range of sample smart cards to be tested, and modifying the probabilities of failure.

An arbitrary ratio of successful PIN and fingerprint is used; it can be modified to allow flexibility in testing different probabilities of failure.

The following is part of the simulation output produced:

```
sender_object:
////////////////////////////////////
sender_object:// Card count: 100
sender_object:// Card ID: 611
sender_object:// Pin entered: correct
sender_object:// entry duration: 1 s
sender_object: ////////////////////////////////////
sender_object: begin transition 1
smartcard_reader_object: begin transition 2
smartcard_reader_object: end transition 2
smartcard_reader_object: begin transition 3
smartcard_reader_object: Good pin
smartcard_reader_object: end transition 3
sender_object: end transition 1
sender_object: *** good pin decoded ***
smartcard_reader_object: begin transition 4
smartcard_reader_object: end transition 4
sender_object: ////////////////////////////////////
sender_object:// Card count: 100
sender_object:// Card ID: 611
sender_object:// Fingerprint entered: correct
sender_object:// Entry duration: 5 s
sender_object: ////////////////////////////////////
sender_object: begin transition 5
smartcard_reader_object: begin transition 6
smartcard_reader_object: end transition 6
smartcard_reader_object: begin transition 7
smartcard_reader_object: end transition 7
smartcard_reader_object: begin transition 8
smartcard_reader_object: end transition 8
sender_object: end transition 5
smartcard_object: begin transition 9
smartcard_reader_object: begin transition 10
smartcard_reader_object: end transition 10
smartcard_object: end transition 9
sender_object: begin transition 11
sender_object: end transition 11
smartcard_object: begin transition 12
smartcard_object: end transition 12
smartcard_object: begin transition 13
smartcard_object: end transition 13
certificate_authority_object: begin transition 14
certificate_authority_object: end transition 14
smartcard_object: begin transition 15
smartcard_object: end transition 15
smartcard_object: begin transition 16
smartcard_object: end transition 16
receiver_object: begin transition 17
receiver_object: end transition 17
certificate_authority_object: begin transition 18
certificate_authority_object: end transition 18
receiver_object: begin transition 19
receiver_object: end transition 19
```

Figure (23): Simulation Output of Transaction Flow in the Smart Card System.

The transitions in the output correspond to the transactions' numbers in the UML diagram in figure (19). Obviously, the designer can observe the attempts to enter the right PIN and Biometric along with the required timing. This allows the testing of the effectiveness of the authentication methods used, by running simulation on different number of smart cards with different probabilities of failure; it is possible to evaluate the effectiveness of each authentication method.

This demonstration is in essence showing the objects along with their related transactions that take place in a smart card system. It is quite meaningful though to demonstrate this diagram, simply because if you cannot simulate it there is no other way of knowing that it is correct.

Testing the proposed authentication methods in the smart card system is the next step, as mentioned previously, one proposed model has the PIN and Biometrics as authentication methods, and the other model proposed two Biometric methods (physical and behavioural).

5.1.4.2 Testing the Authentication Methods

Validation of the authentication methods in the smart card system is based on two proposed models. The first model utilises the PIN and Biometrics authentication methods, while the second model utilises two Biometrics authentication methods (a physical and a behavioural method).

The main reason behind carrying out these correctness tests is to check that the simulation using the executable model is actually working. Other purposes behind conducting these correctness tests encompass the following:

- Confirmation of the functionality/workability of the smart card simulation tool and the availability of test results.
- Reliability of the smart card simulation tool in which actual results through the simulation are obtained.
- The degree of flexibility of assigning thresholds and failure probabilities, which will assist in customising the simulation tool based on the industry and sector in which the smart card system will be used.
- The speed of testing, which allows users of the simulation tool to obtain results and manipulate thresholds with ease and flexibility.

The following tests have been performed:

Test #1: Examination of the use of PIN and Biometrics as authentication methods.

Test #2: Examination of the use of two Biometrics techniques as authentication methods.

For each of these tests, an arbitrary probability of failure has been assigned to each of the authentication methods. For example, the probability of failure for the PIN is set at 15%, for the Biometrics (fingerprint) it is set at 10%, and the time allowed for entering the correct pin and correct fingerprint is set at 10 seconds for each. These probabilities are just examples that have been set while taking into consideration potential user errors, system errors, environmental factors, and the possibility of successful attacks during the process of using the smart cards.

The reason for assuming that the PIN has a slightly higher probability of failure is based on the findings explained in earlier sections of the thesis. The

PIN authentication method is weaker than the Biometrics and thus there is a higher probability of successful attacks and user errors and mistakes.

Test #1 – PIN and Biometrics:

Table (13) provides a summary of the testing process and its results for the first model:

Remarks	Number of simulated smart cards						
	100	**500**	**1000**	**1500**	**2000**	**2500**	**3000**
good pin decoded	100	500	998	1490	1976	2464	2950
pin incorrect/re-enter correct pin	16	102	207	302	394	493	587
timeout error (pin)	9	58	125	189	257	299	376
good bio decoded	100	500	998	1490	1976	2464	2950
bio incorrect/re-enter correct bio	13	38	82	126	167	200	234
timeout error (bio)	11	58	124	171	236	299	359

Table (13): Results from Testing the PIN and Biometrics Authentication Methods.

Testing was based on using a sample starting at 100 smart cards and up to 3,000 cards to provide the necessary range and spectrum for testing. Table (13) displays the results for both the PIN and Biometrics authentication methods based on the 3 scenarios of potential failure/error.

An examination of the results may be interpreted according to the industry and sector of use which dictate the levels of acceptable thresholds and probabilities of failure.

Initially, when examining the relationship between the expected and observed results of failure attempts across all sample sizes we are able to confirm that it is a linear relationship and that observed failure attempts are always below the expected range.

The following are graphs that show the total expected and observed attempts of failures of PIN and Biometrics that are recorded as a result of the test.

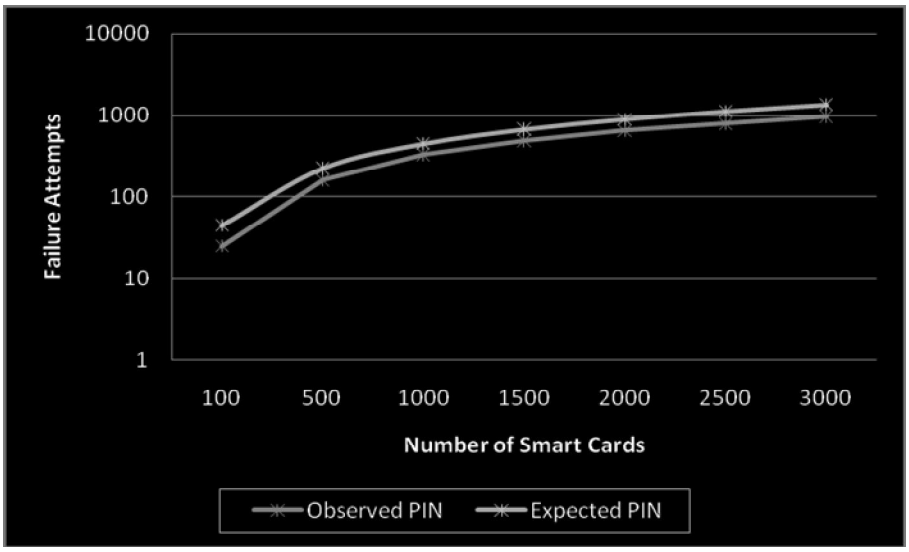

Figure (24): Expected and Observed PIN failure attempts in PIN and Biometrics proposed model.

The graph also concludes that the higher the number of smart cards tested, the smaller the variance between the expected and observed failure attempts. In a sample size of 3,000 cards, failure attempts are 963; over 30% of the sample size. This failure percentage alerts us to the vulnerability of the system indicating that both the user and the system will operate in a risky environment.

This entails a low level of acceptance of usage from both parties due to the increased risks represented by the use of this method. Having such a high degree of risk and vulnerability in the system will expose it to numerous additional threats from different sources.

Figure (25) demonstrates the expected and observed failure attempts using the Biometrics authentication methods. The probability of failure used in testing the Biometrics method is arbitrary, the earlier sections of the thesis discussed the authentication methods in details, and the result of the discussions showed that the Biometrics authentication method is stronger than the PIN, hence the

probability of failure assigned to the Biometrics method in this test is 10%, which is less than the PIN authentication method by 5%. Upon examination of the expected and observed failure attempts of the Biometrics authentication methods the results are contrary to those of the PIN authentication. Most specifically, when simulating a sample size of 3,000 smart cards the number of recorded failure attempts is reduced to 593; about 20% of the sample size. This reduction of 10% in failure attempts provides a good indication of the strength of the authentication method employed.

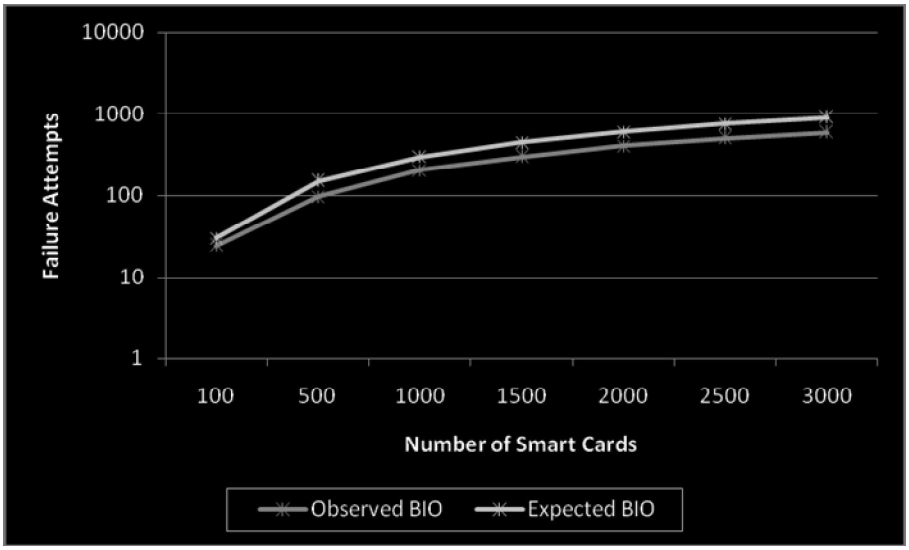

Figure (25): Expected and Observed Biometric Failure Attempts in PIN and Biometrics Proposed Model.

The results of the expected and observed PIN and Biometric failure attempts are listed in table (14) below and recorded as percentage of the total sample size:

Number of Smart Cards	**100**	**500**	**1000**	**1500**	**2000**	**2500**	**3000**
Percentage Observed (PIN)	8%	11%	11%	11%	11%	11%	11%
Percentage Expected (PIN)	15%	15%	15%	15%	15%	15%	15%
Percentage Observed (BIO)	8%	6%	7%	7%	7%	7%	7%
Percentage Expected (BIO)	10%	10%	10%	10%	10%	10%	10%

Table (14): Percentages of Expected and Observed PIN and Biometrics Failure Attempts.

When comparing the observed PIN failure attempts to the Biometrics failure attempts, it is noted that the percentages are 10% and 7%, respectively. Although the variance is relatively minor, it indicates that the PIN authentication method requires additional monitoring, particularly in avoiding risks of external threats that pose potential harm against the users and system confidentiality and privacy.

Furthermore, under the simulation of 1,000 smart cards, it is noted that two cards have been banned due to reaching the maximum attempts of PIN entry. However, as the sample size increases, the number of banned smart cards grows exponentially as illustrated in the graph below.

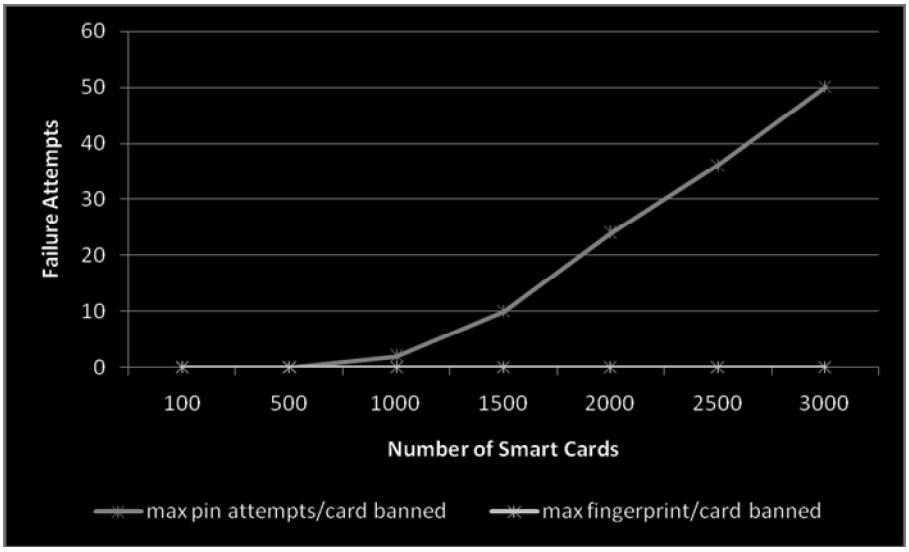

Figure (26): Smart Cards Banned in PIN and Biometrics Proposed Model.

For example when running 3000 smart cards, about 50 of them were banned during the PIN authentication step, on the contrary, for the Biometrics authentication method, it is noted that no smart cards have been banned when using this method. Thus, the example of giving lower probability of failure to the Biometrics authentication method in the test gives results that indicate that the

use of Biometric authentication method provides better security levels when adopted by smart cards, particularly ones that store and have access to sensitive data.

Test #2 – Two Biometrics:

The second test examines the second proposed model which combines two Biometrics authentication methods. The probabilities of failure that are assigned to both Biometrics methods are 10%. The following are the recorded results of the attempts that took place during the test:

Remarks	Number of simulated smart cards						
	100	**500**	**1000**	**1500**	**2000**	**2500**	**3000**
good bio1 decoded	100	500	994	1484	1999	2499	2998
bio1 incorrect/re-enter correct bio1	11	49	107	170	197	253	301
timeout error (bio1)	11	49	123	175	218	277	342
good bio2 decoded	100	500	994	1484	1999	2499	2998
bio2 incorrect/re-enter correct bio2	12	65	119	169	253	303	363
timeout error (bio2)	9	66	121	175	274	321	393

Table (15): Results from Testing Two Biometrics Authentication Methods.

Compared to the results of Test #1, the results of this test provide more acceptable results due to the reduced observed results of failure attempts of the Biometrics authentication method. Overall, this allows for operating the smart cards in a safer and more secure environment, particularly when it comes to storage and access of sensitive information.

As illustrated in figure (27), all observed attempts are within an acceptable range, more specifically below the expected failure attempts. It is worth noting that based on the requirements of the industry and sector in which the smart card will be deployed; system administrators are able to set suitable thresholds and failure probabilities.

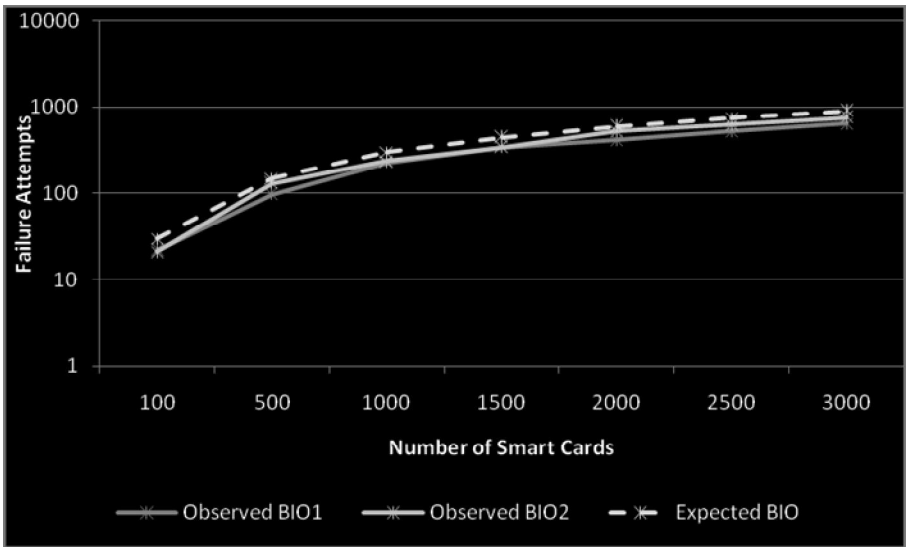

Figure (27): Expected and Observed Biometrics Failure Attempts in Two Biometrics Proposed Model.

A preliminary judgment of these results indicate that the use of two Biometric authentication methods will further strengthen and protect the authentication process and provide an additional level of security and confidentiality.

Number of Smart Cards	100	500	1000	1500	2000	2500	3000
Percentage Observed (BIO1)	7%	7%	8%	8%	7%	7%	7%
Percentage Expected (BIO1)	10%	10%	10%	10%	10%	10%	10%
Percentage Observed (BIO2)	7%	9%	8%	8%	9%	8%	8%
Percentage Expected (BIO2)	10%	10%	10%	10%	10%	10%	10%

Table (16): Percentages of Expected and Observed Biometrics Failure Attempts.

The average of failure attempts in the first Biometrics authentication method is 7%; while the second method has an average of 8% failure attempts. Taking this information along with the number of banned cards as illustrated in figure (28) provide us with several observations. Firstly, the use of two Biometrics authentication methods provides a rigorous means of security for users and administrators of smart cards. The added level of security indicates that if the

first Biometrics authentication was attacked, the second Biometrics authentication will make it difficult to conduct a second attack.

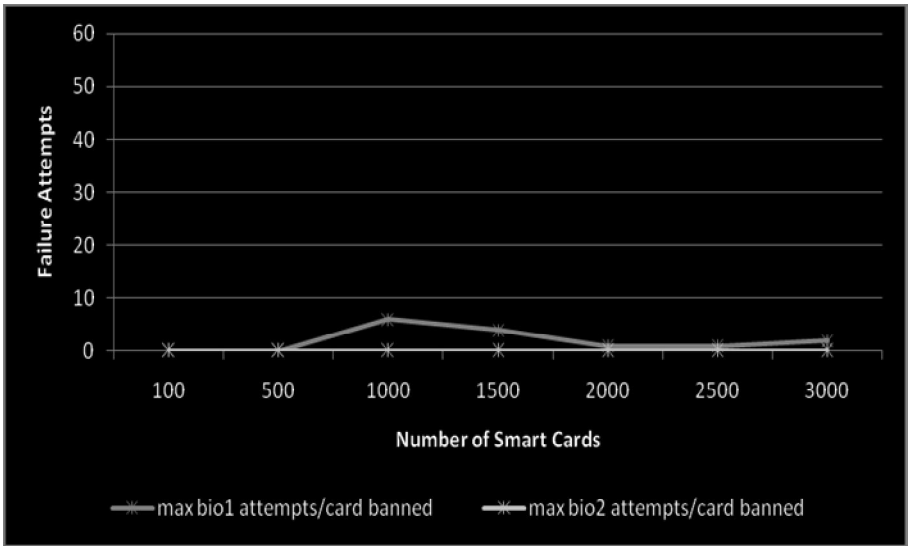

Figure (28): Smart Cards Banned in Two Biometrics Proposed Model.

The second observation takes into consideration the number of banned smart cards during this testing model. The most number of banned smart cards was present when simulating a sample size of 1,000, where 6 cards were banned. However, when simulating a sample size of 3,000 cards, this number is reduced to 2 cards only. This concludes that not only is this method more robust than the previous model, but it also allows for a safer processing environment even at high transaction volumes. Although the probabilities of failures used in conducting the tests are just examples, yet the outcome shows that the executable model used to test the authentication methods is working, which is the main purpose of carrying out the tests.

Having examined the two test results and concluding that the use of two Biometrics authentication methods are more powerful, robust and safe as

opposed to the use of PIN and Biometrics combined, to adopt such method in real life it is important to assess the usability of such practice.

For example, when using the smart card for conducting a bank transaction or as means of identification, the frequency of use dictates the simplicity and flexibility of authentication methods. Customers using smart card based banking cards are unlikely to accept using two Biometrics authentication methods every time they wish to conduct a bank transaction. As such, it was decided to manipulate the methods of Test #1 where the two methods were reversed in sequence; the Biometrics authentication method will be conducted before the PIN entry.

Test #3 – Biometrics and PIN:

The initial expectation is that the use of a Biometrics authentication first will decrease the possibility of failure attempts and attacks. This mechanism supports the security concept of using something you own (smart card), something you are (Biometrics), and something you know (PIN). The results of the test are listed below:

Remarks	**Number of simulated smart cards**						
	100	**500**	**1000**	**1500**	**2000**	**2500**	**3000**
good bio decoded	100	500	1000	1499	1999	2499	2993
bio incorrect/re-enter correct bio	13	38	83	126	162	199	236
timeout error (bio)	9	56	122	176	244	307	363
good pin decoded	100	500	1000	1499	1999	2498	2991
pin incorrect/re-enter correct pin	17	103	207	305	412	507	617
timeout error (pin)	11	60	129	190	259	306	385

Table (17): Results from Testing the Biometrics and PIN Authentication Methods.

The probabilities of failure set in this test are similar to the first test, where the probability of failure for Biometrics is 10% and PIN is 15%. The only

difference is that the Biometrics authentication will be conducted before the PIN authentication. As illustrated in table (17) above, there are fewer errors during the first authentication level which translates to a more secure process at the initial stages of this process. This method has automatically reduced the number of potential attacks on the system and will therefore reduce potential attacks at the second authentication level.

The results of this test have been plotted and illustrated in figures (29) and (30). The number of observed failure attempts at the Biometrics authentication method range between 22 and 599 for sample sizes of 100 and 3,000 smart cards consecutively. At the PIN authentication level, observed failure attempts are recorded at 28 and 1,002 for sample sizes of 100 and 3,000 smart cards consecutively. Although the observed failures at PIN level are high, it is important to note that we start off with a more rigorous and secure process with the use of the Biometrics authentication.

Figure (29): Expected and Observed Biometrics Failure Attempts in Biometrics and PIN Proposed Model.

This ensures that the process is faced with less failure attempts and potential attacks, which will drop down to the second authentication level which uses the PIN.

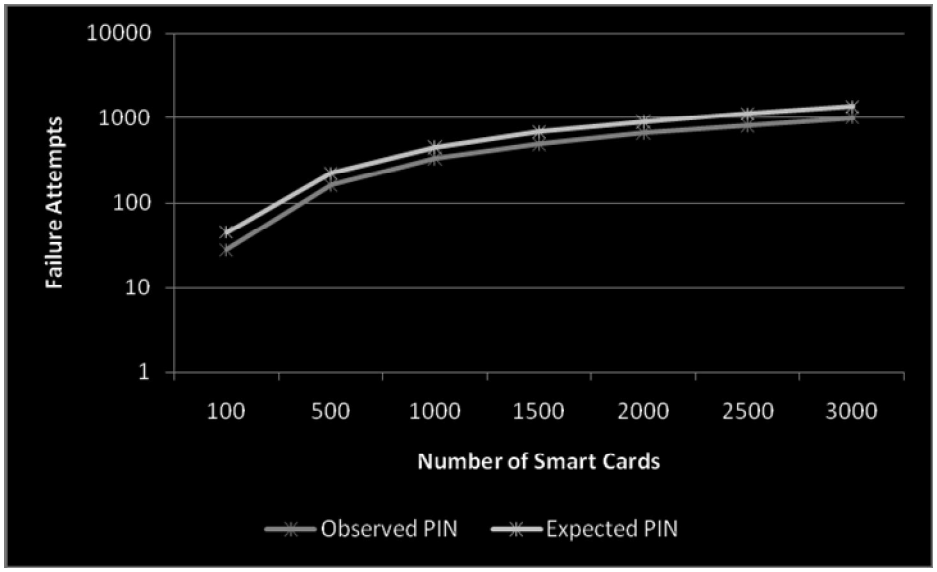

Figure (30): Expected and Observed PIN Failure Attempts in Biometrics and PIN Proposed Model.

Therefore, when deciding on the use of two authentication methods, it is recommended that a Biometrics authentication is used as a first level of defence, followed by the usual authentication method of inputting a PIN.

Number of Smart Cards	**100**	**500**	**1000**	**1500**	**2000**	**2500**	**3000**
Percentage Observed (BIO)	7%	6%	7%	7%	7%	7%	7%
Percentage Expected (BIO)	10%	10%	10%	10%	10%	10%	10%
Percentage Observed (PIN)	9%	11%	11%	11%	11%	11%	11%
Percentage Expected (PIN)	15%	15%	15%	15%	15%	15%	15%

Table (18): Percentages of Expected and Observed Biometrics and PIN Failure Attempts.

Putting these recommendations into table (18) demonstrating percentages of failure attempts, we note that the average observed Biometrics failure attempts is 7%, while the average of observed PIN failure attempts is 11%. This confirms our assumptions that the first level of defence is strong and will decrease the

number of illegitimate users that may potentially attack the system during the process.

The final confirmation that this test produces the best security level and least failure attempts is examining the number of banned smart cards as illustrated in figure (31).

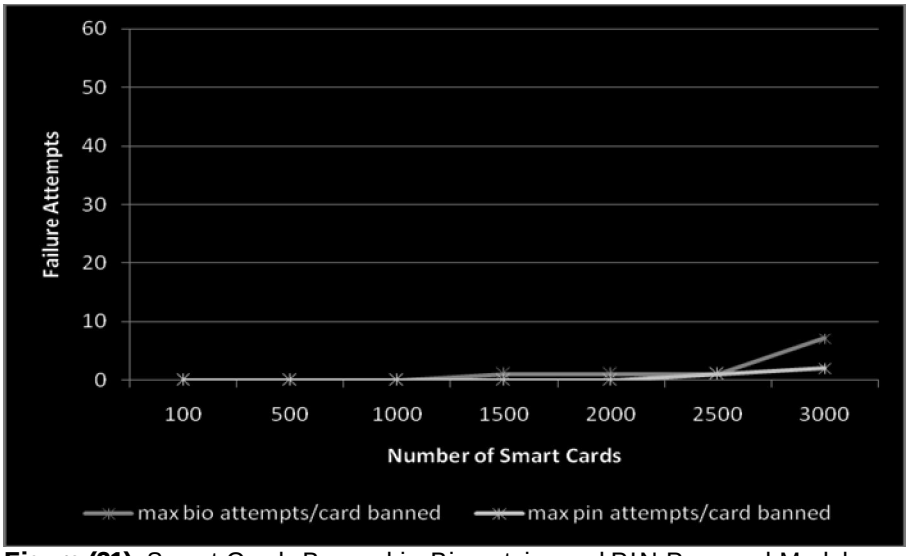

Figure (31): Smart Cards Banned in Biometrics and PIN Proposed Model.

When using the Biometrics authentication method before the PIN, the number of banned smart cards is recorded at 7 and 2 consecutively for a sample size of 3,000 smart cards. This comes low compared to when the PIN is used prior to the Biometrics where the number of banned smart cards was 50 and 0 consecutively for a sample size of 3,000.

Given the benefits to the user and administrator, as well as the practicality of using the Biometrics and PIN authentication methods across most industries, it is recommended to adopt this method in the given order as it proves to provide the best security levels.

5.1.4.3 Simulating Attacks on the Smart Card System

As discussed in chapter (3), section 3.1.3, there are different types of attacks that have different probabilities of occurrence and different consequences on the smart card system and its users. Each attack targets different areas of the system and has a specific goal; this section is concerned about the attacks that are practised while the smart card is in use. Some of the attacks violate the smart card system authentication, privacy, and confidentiality like attacks on PIN or attacks on Biometrics. Other attacks violate the smart card system integrity, reliability, availability, and even authentication like invasive attacks, side channel attacks, etc. Please refer to Appendix (B).

Figure (32) is a UML sequence diagram that demonstrates the types of attacks that may occur in any smart card system, even though safeguards and controls like PIN, Biometrics, and PKI are in place.

The purple callouts represent the types of possible attacks that an attacker can carry out in that area precisely; in addition, the red callouts represent the attacks that are created in the executable model to test the system's robustness.

The executable model allows us to simulate attacks on the system. An attack on any part of the system is essentially another transaction inserted into the model. For example, to simulate an attack that allows the attacker to steal the private key released from the smart card object, which is coded as a state machine, an attacker is implemented as a singleton class that can intrude into multiple simulation modules in a thread-safe manner.

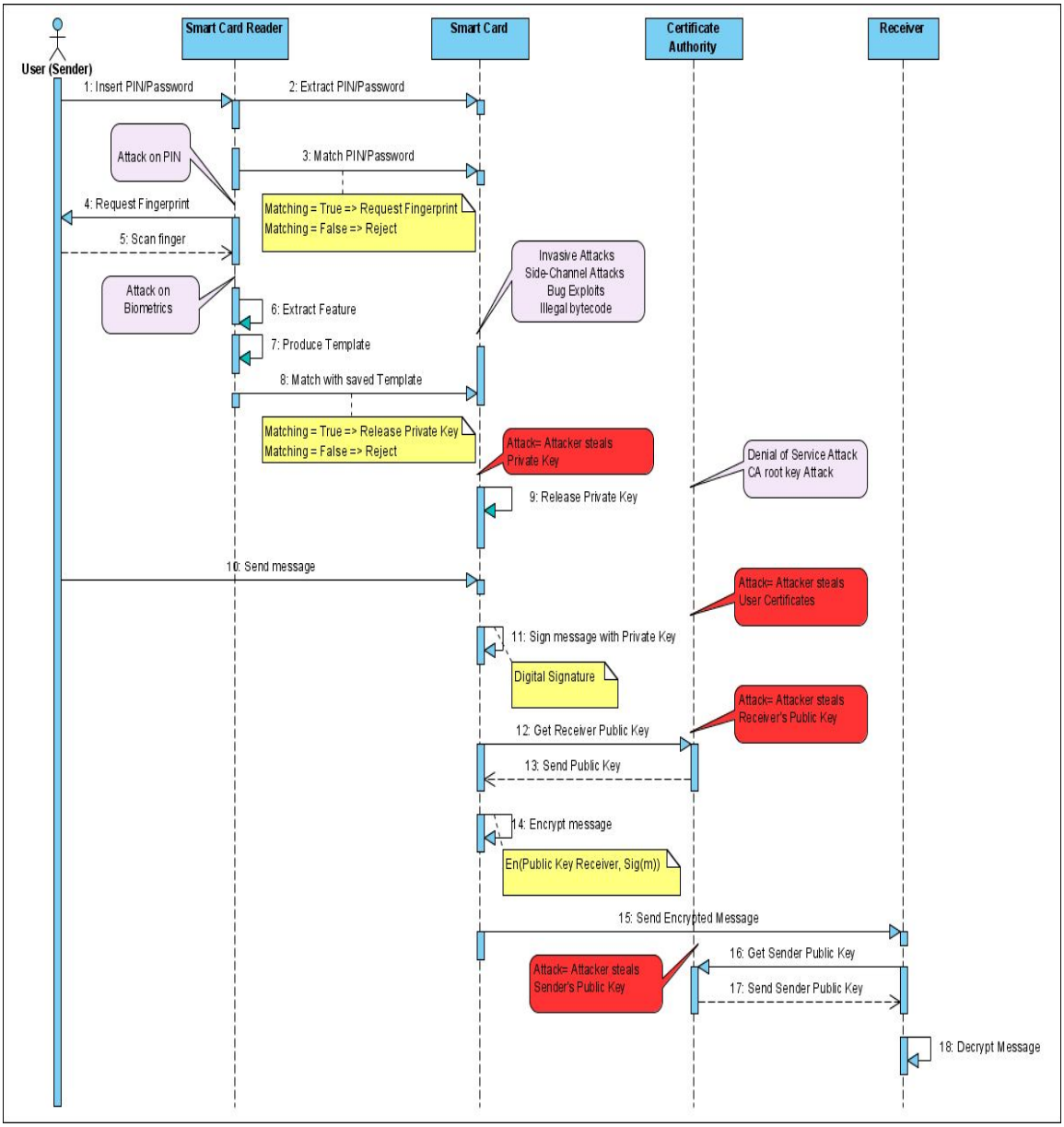

Figure (32): Sequence Diagram- Possible Attacks on PIN, Biometrics (Fingerprint), and PKI Smart Card System.

The attack is defined at the beginning of the model, and then a transaction is effectively inserted into the model by including the following line of code at the appropriate point in the Smart Card module:

```
attack::getInstance().set_private_key(private_key);
```

Now, the model waits for transitions 1 to 8 to occur, and then the attacker interferes and attacks the system after transition 8 where the private key is released.

```
////////////////////////////////////
sender_object:// Card count: 98
sender_object:// Card ID: 547
sender_object:// Pin entered: correct
sender_object:// entry duration: 7 s
sender_object: ////////////////////////////////////
sender_object: begin transition 1
smartcard_reader_object: begin transition 2
smartcard_reader_object: end transition 2
smartcard_reader_object: begin transition 3
smartcard_reader_object: Good pin
smartcard_reader_object: end transition 3
sender_object: end transition 1
sender_object: *** good pin decoded ***
smartcard_reader_object: begin transition 4
smartcard_reader_object: end transition 4
sender_object: ////////////////////////////////////
sender_object:// Card count: 98
sender_object:// Card ID: 547
sender_object:// Fingerprint entered: correct
sender_object:// Entry duration: 6 s
sender_object: ////////////////////////////////////
sender_object: begin transition 5
smartcard_reader_object: begin transition 6
smartcard_reader_object: end transition 6
smartcard_reader_object: begin transition 7
smartcard_reader_object: end transition 7
smartcard_reader_object: begin transition 8
smartcard_reader_object: end transition 8
sender_object: end transition 5
Attacker initialized, @104 s
Attacker stole the private key, @104 s
smartcard_object: begin transition 9
smartcard_object: end transition 9
```

Figure (33): Simulation Output of Attack on Private Key

The output of the simulation with an attack shows that the attacker gets hold of the private key by practising a successful attack on the smart card object.
In this example, the attacker has to conduct one of the physical or logical attacks that were explained in details in chapter (3), section 3.1.3, to be able to get hold of the private key, so the attacker can practise a successful side channel attack, invasive attack, attacks during PIN comparison, or attacks on Biometrics. The executable model in this study does not simulate the physical or logical attack; it

only assumes that a physical or logical attack has taken place. For that reason, it simulates an attack and creates an attacker class with features that allow the attacker to modify the transitions and as a result gain access to the user's secret information, specifically the private key.

In essence, the attacker being able to get hold of the private key is the worst case scenario. When the attacker steals the private key, the user will be in a very critical situation because the attacker can claim to be the legitimate user to the system and gets access to all the privileges of the legitimate user. The whole idea in the key management security is to secure the private key; it is the most important element to be kept in a highly secured place. This successful attack indicates a weakness in the protocol used within the smart card system.

Another example of utilising the executable module in attacks simulation is by modeling another sort of an attack, which is carried out on the key exchange operation. This time the attacker monitors the public keys exchanged between the users and the CA, and gets hold of the users' public keys. Being able to interfere with the key exchange protocol opens a door for the attacker to practice attacks that result in network disruption and loss of user trust like for example carrying out a man-in-the-middle attack [159], or a multi-protocol attack [160]. Although the public keys are available to everyone, the attacker can still monitor the key exchange messages between the sender and the receiver without both of them knowing, and then the attacker can use the public keys of both users in a way that convinces them that they are exchanging messages with each other

without someone in the middle, for more information about the details of man-in-the-middle-attack on public keys please refer to [161] and [159].

```
smartcard_object: begin transition 13
certificate_authority_object: begin transition 14
certificate_authority_object: end transition 14
Attacker stole the receiver public key, @203 s
smartcard_object: end transition 13
smartcard_object: begin transition 15
smartcard_object: end transition 15
smartcard_object: begin transition 16
smartcard_object: end transition 16
receiver_object: begin transition 17
certificate_authority_object: begin transition 18
certificate_authority_object: end transition 18
Attacker stole the sender public key, @206 s
receiver_object: end transition 17
receiver_object: begin transition 19
receiver_object: end transition 19
```

Figure (34): Simulation Output of Attack on Public Keys

This example focuses on modeling an attack that allows the attacker to interfere through the transactions exchanged between the user and the receiver and gets hold of the data exchanged without both of the users knowing, by being able to model the attack, it is possible to point out a gap in the protocol that allows an attacker to monitor the flow of data, interfere within the transactions, and get hold of the public keys exchanged.

Attacking the key exchange operation generally and stealing the private key specifically violates the confidentiality, privacy, authentication, and integrity properties of the system. Also, it compromises the security of the user, which may result in identity theft, information leakage, or message alteration. Being able to steal the private key points out vulnerability within the security protocol employed in the system.

A Denial of Service (DOS) attack is simulated using the same model. The attack aims at violating the availability property of the system security. The

DOS attack takes place against the Certificate Authority server and manifests through the following mechanism. First, the attacker attempts to exhaust the server through high frequency login requests. The aim is to guess user pin or passwords to gain unauthorized access into the smart card system. When successful, the attacker intrudes into the certificate authority and intercepts the user certificates and sender/receiver public keys. Due to such attack, the smart card server fails to provide the services to legitimate users. Figure (35) shows result of DOS attack simulation:

```
iteration: 4 at time: 2 s
insert_pin_password
extract_pin_password
request_fingerprint
match_with_saved_templates
release_private_key
release_private_key
send message
get_receiver_public_key
send_encrypted_message
Attacker stole the sender public key,
SERVICE DENIED, @2 s
```

Figure (35): Simulation output of Denial of Service Attack

As can be seen, the transactions of the smart card system are running normally, however, when the DOS attack successfully takes place, the service is denied and the attacker gets hold of the users public keys exchanged among the system objects. In addition, the subsequent transactions failed to occur because the Certificate Authority server is unavailable. This attack shows that the availability property has been violated; the system users are going to suffer from service unavailability, and will not be able to use their smart cards until the Certificate Authority server recovers from the attack.

DOS attacks are indistinguishable from legitimate sign-in requests. The only differentiation is in the frequency of sign-in attempts and their origin. A large

number of sign-in attempts in rapid succession can be indicative of a DOS attack. Hence, smart card systems can be protected from DOS attacks by identifying high frequency of login attempts from a source and denying service to the source of such attack. Another effective way is to limit the number of login attempts a user is allowed at a time.

5.2 Concluding Remarks

In summary, the executable model developed using SystemC TLM allowed the designer to test the proposed models that support a combination of authentication methods; by running simulations on different number of smart cards with different authentication methods and recording the results, the designer can examine the robustness of the proposed models in terms of enhancing security specifically during the phase of authenticating the smart card system users.

The simulation tool provided a quick, automated, and flexible environment to test the proposed models, in addition to allowing the designer to observe and modify the transactions whenever changes are required.

In addition, the SystemC TLM executable model also allowed the designer to discover the weak points of the system and point out vulnerabilities; the successful attacks indicate that there are weaknesses in the security protocol. By referring to table (4) in chapter (3), which shows the service phases and the related types of security requirements in the smart card system, the executable model included two authentication methods, which are PIN and Biometrics, and one cryptographic key exchange mechanism that is PKI to be able to achieve the

security goals that are listed in table (4). However, by running the tests on the authentication methods, and carrying out successful attacks that were explained in details in chapter (3) like attacks on PIN, attacks on Biometrics (figure (7)), and other physical and logical attacks on the proposed model, some of these security goals have been violated.

Testing the proposed model against physical and logical attacks while the smart card is in use has resulted in giving the attacker the chance to get hold of the user's private key, and therefore violating numbers of security properties like authentication, confidentiality, privacy, and integrity. Also, by successfully simulation a denial of service attack (DOS), the attacker succeeded in interpreting the key exchange mechanism and denying the service to the legitimate users, which resulted in violating the availability and reliability security goals. This in essence shows that the system is vulnerable to threats and successful attacks taking place. Yet, to be able to reduce the probability of successful attacks, the executable model allows the designer to modify the executable model to test against future attacks.

In contrast with the UML diagram, the animation makes it possible to see the attack actually happening. Furthermore, it is possible to make changes easily within the model and try number of attacks to test the system robustness by simply inserting transactions into the UML diagram, and transforming it into transactions within the SystemC TLM executable model.

To be able to defend the smart card system against possible attacks, some countermeasures are suggested. The countermeasures that can be implemented to prevent invasive attacks are within the design of the chip, such as tamper

resistant topological design measures. Some integrated circuits include an active shield or sensor that detects an attack when its lines are cut or contacted, if an attack takes place the shield erases the chip's memory and ends all functions, which ends up making the smart card unusable [100]. Yet, not all types of smart cards have this type of tamper resistant chips; hence, it is vital to make sure that the chip used is a silicon tamper resistant chip to be able to reduce the possibility of invasive attacks taking place.

To prevent side channel attacks, suggested countermeasures by [100] are randomness of behaviour, which is achieved by manipulating data in a way that the value presented in the memory is always masked with a random value to prevent interpretation of leaked information. Other countermeasures are memory layout scrambling, memory address bus encryption, noise generation, traffic adding/padding, time disturbance and algorithmic process masking. In addition, redundancy and protecting the values stored in the memory with a checksum may also contribute to preventing fault analysis.

To be able to defend the smart card systems against DOS attacks, countermeasures like identifying high frequency of login attempts from a source and denying service to the source of such attack is an effective way, another way is to limit the number of login attempts a user is allowed at a time.

To conclude, the executable model can give the designer the opportunity to simulate countermeasures that are programmable by SystemC and TLM. Nonetheless, changing the design of the integrated circuits is not within the capabilities of the executable model and it is outside the scope of this study.

Chapter 6

Conclusions and Future Work

6.1 Conclusion

The e-business environment is expanding quickly; a large portion of government and business offices in advanced countries are adopting the paperless office concept. The smart card is the latest trend in the e-business environment, particularly within the e-government and e-banking systems. Along with the advances and benefits of each technology there are associated risks that may have a negative impact on the system, which may lead to system failure. Today, governments that deploy the smart card system are having various applications activated in the e-government system and accessed by number of users through smart identification cards. This raises a huge security responsibility that the management of the whole information system has to fulfil.

In addition, other types of organisations are also employing the smart card for different usages; these cards are being used as banking cards, loyalty cards, prepaid cards, etc. Applying the risk management programme is imperative to be able to effectively manage the system. Such risk management programme provides governments and organisations with a clear idea about the assets of the system along with their values, threats identification, vulnerability identification, the required security issues and goals like (confidentiality, authentication, integrity, non-repudiation, etc), risk determination, and risk

mitigation. The final and very important step of the programme is concerned about applying the best safe-guards that will mitigate the associated risks in addition to number of controls to allow better management and backup to the system.

Each of the various types of the smart card system determines its unique probability of attacks and severity of related consequences. Taking the risk analysis into consideration, it is notable that the results indicate that using the smart card as a banking card or an identification card is extremely risky due to the sensitivity of information and value of transaction being processed. The probability of attacks and the severity of the attacks to this type of cards may cause severe harm to the system and its users. Governments and organisations must therefore focus on reducing potential risks to the system by applying the best technology to secure the system assets. Thus, going through the risk management programme will assist governments and organisations to avoid negative impacts on the system along with reducing the risks to an acceptable level by employing the best available safe-guards such as PKI and Biometrics. This in turn will lead to gaining users' trust, loyalty, and confidence, which will boost usage and adoption of smart card system beyond its current boundaries.

The risk analysis in this study focuses on the smart card system, which is something that has never been done before. Most risk management programmes are concerned about information technology security in general, but there has been no risk analysis study or guide that is conducted specifically on smart cards.

Data storage in the smart card system must be properly and effectively managed. Additionally, the security methods or safeguards employed must also be divided into levels bearing in mind that each type of smart card requires different security methods at different levels and stages. As a result, designing the smart card, deciding what types of applications the card is serving, and employing the security methods are critical stages in the smart card life cycle.

From a modelling and design perspective, modelling provides ways to join security engineering with software engineering; this manages the complexity of the systems by offering a visualised way of looking at systems entities and functions. Modelling each transaction that occurs while using a smart card is very important; it assists the designer of the system to identify the occurrences where security properties must be activated to avoid potential system attacks.

After designing the model, testing was carried out to be able to determine the weaknesses of the model and to exploit the vulnerabilities of the proposed system. Determining the vulnerabilities in the design phase of the system reduces the risks that may occur during the system implementation.

The UML diagrams along with their extensions are an ideal form of modelling the systems; they have features that enable the designer to visualise the whole process and its sub-transactions. UML diagrams were used to model the smart card system protocol and processes, and present the transactions that take place while messages are exchanged during the registration and verification processes. In addition, the UML diagrams allowed the designer to identify areas that may be vulnerable to attacks. This part of the study has been published in a

conference paper in the 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing; please refer to Appendix (B).

One of the drawbacks of UML, however, is that it does not allow the designer to see what happens if something goes wrong with the system; it only demonstrates the way things should work. Therefore, the importance of simulation arises to enable the designer to oversee the whole process and repair any issues or problems that occur. By creating an executable model of a smart card system, including the security protocols and transactions, it is possible to examine the strengths and determine the weaknesses by running tests on the model.

SystemC TLM was used to provide a simulation tool; it transformed the UML static model into an executable model. The executable model provided the opportunity to see the transactions flow within the system objects in an animated manner. It also gave the designer the ability to carry out tests to be able to examine the authentication methods that are proposed by the designer to be employed in the smart card system; this work has also been published in the conference paper presented in the 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. The tests' results demonstrated the number of failure attempts in each authentication method, which helped the designer identify the strengths and weaknesses of the employed methods. It also indicated that the order of the authentication methods that are used determines the level of security provided by the system, which is a critical point to be looked at. After having tested the proposed models that include two authentication methods, PIN and Biometrics, the outcome was more favourable when the user

submitted the Biometrics evidence before the PIN. Additionally, there were less smart cards banned during this test, which gives a clear indication that this mechanism should be adopted to ensure confidence and security for both the smart card user and system administrator.

The executable model allowed the simulation of different types of attacks in different parts of the system. The results showed that number of security objectives like confidentiality, authentication, integrity, and availability were violated; hence, identification of the system weaknesses and vulnerabilities can be pointed out. As such, the benefits of building an executable model include allowing the designers to have a clear view of the weaknesses in the security requirements, methods, and protocols used in the smart card system. This, in turn, allows adaptation of various usages of the smart card system in different business environments where security and authenticity requirements vary. This executable model is a new way of modelling the smart card system, which has not been done before, this in turn is considered as an additional contribution that supports bridging the gap between the design and implementation phases of the smart cards systems' development.

6.2 Future Work

The future work at this point is going to look at the current problem from different angles. According to the in-depth reading and data gathering of how the data are stored in the smart card, where the data are stored, the ways to have access to these data, and the way these data are secured. It appears that each type of smart card varies in the way the data and information are stored,

accessed, and protected. After carrying out the risk management program, the results came out with different levels of risk associated with each type of smart card. It really depends on the applications that the smart card is responsible of handling. Each application requires different amount of information to be stored in the smart card; therefore, requires different types of security methods to be implemented to better secure the information stored. The results show that the banking card has an undesirable level of risk, besides, the identification smart card also scored a high risk rate among other types, the risk associated with this type of card is considered to be undesirable also. This indicates that these particular types of smart cards require more attention than others.

Building a prototype out of the proposed models, and examining the usability of the system, the people's acceptance of using this type of technology, and their willingness of having it on their daily routine is a valuable idea. People's perception and willingness to use the better secured technology that requires more effort and time to be given by the user is something important to look at. It brings in mind the question of: what if we are trying to come up with the best way of securing the smart card but this way can end up being rejected by the actual users? This result will affect the technology in a very bad way. It simply means that if the users have not appreciated the new way of using the smart card, then there is no use of applying the proposed security methods. Evaluating the usability of the smart card with more security procedures, where the user must go through more authentication steps while using the smart card is the next step. In computer science and human-computer interaction, usability is a term that is used to indicate the ease of employment of a particular computer

program, interface, or device. It is concerned with how efficient, easy to learn, satisfying, and less error contained the technology is. Thus, in order to evaluate the usability of the proposed model and the prototype built, a sample of users have to be picked and use the demonstrated prototype, then their opinions and reflections towards the usage of this model have to be examined by distributing a questionnaire that contains number of questions, which are concerned with the usability and acceptability of the model. In fact, it is quite imperative that the users perceive the smart card with more sophisticated security methods to be usable, acceptable and reliable.

Also, future work can utilise the executable model produced in this study; it is a very useful simulation tool because it is automated, flexible, allows high speed simulation, and is easy to use. It allows the designers to run more tests and examine more authentication methods and key exchange mechanisms, or practice more types of attacks and record the results. The designers can even suggest new controls and safeguards and add them to the executable model, then run some tests to evaluate the strengths and weaknesses of the suggested controls and safeguards.

Chapter 7

References

[1] Microsoft Corporation. (2005). *X.509 Technical Supplement* [Online]. Available: http://msdn.microsoft.com/en-us/library/aa480610.aspx

[2] "Ingenico and Sagem Securite join electronic payment activities, making Ingenico world leader," *Card Technology Today,* vol. 19, pp. 1, 3, 2007.

[3] E. Turban, D. King, J. K. Lee, and D. Viehland, *Electronic commerce 2004: a managerial perspective*. Great Britain: Pearson Prentice Hall, 2004.

[4] S. Liu and M. Silverman, "A practical guide to biometric security technology," *IT Professional,* vol. 3, pp. 27-32, 2001.

[5] eGovernment Portal. (2006). *Bahrain Electronic Government Portal* [Online]. Available: https://www.e.gov.bh/pub/wps/portal/!ut/p/.cmd/cs/.ce/7_0_A/.s/7_0_2E8/_s.7_0_A/7_0_2E8

[6] Bahrain Gateway. (2008). *Airport E-Gate to Ease Travel* [Online]. Available: http://www.bahraingateway.org/index.cfm?fuseaction=document.home&id=479

[7] Portal of Dubai Government. (2010). *eGate Card for Dubai & Abu Dhabi* [Online]. Available: http://www.dubai.ae/en.portal?topic,Article_000551,1,&_nfpb=true&_pageLabel=home

[8] G. Kardas and E. T. Tunali, "Design and implementation of a smart card based healthcare information system," *Computer Methods and Programs in Biomedicine,* vol. 81, pp. 66-78, 2006.

[9] Health e-card. (2010). *Your medical records in your hands* [Online]. Available: http://www.healthecard.co.uk/Patients/tabid/76/Default.aspx

[10] G. F. Anderson, B. K. Frogner, R. A. Johns, and U. E. Reinhardt, "Health Care Spending And Use Of Information Technology In OECD Countries," *Health Affairs,* vol. 25, pp. 819-831, May 1, 2006.

[11] S. e. Canard and H. e. Sibert, "How to fit cryptographic e-voting into smart cards," *Fundamenta Informaticae,* vol. XXI, pp. 1001–1012, 2001.

[12] R. Anderson, *Security Engineering: a guide to building dependable distributed systems*. New York: Wiley, 2001.

[13] "Card Payments Roadmap in the U.S.: How Will EMV Impact the Future Payments Infrastructure?," Smart Card Alliance, Princeton Junction, NJ, Rep. PC-11001, 2011.

[14] Smart Card Alliance. (2010). *EMV Chip Cards Expected for Upscale U.S. Cardholders* [Online]. Available: http://www.smartcardalliance.org/pages/publications-emv-chip-cards-expected-for-upscale-us-cardholders

[15] National Institute of Standars and Technology. "NIST Releases Guide for Applying the Risk Management Framework to Federal Information Systems," NIST, Gaithersburg, MD, Rep. 800-37, 2010.

[16] Z. M'Chirgui, "Smart card industry: a technological system," *Technovation,* vol. 25, pp. 929-938, 2005.

[17] K. M. Shelfer and J. D. Procaccino, "Smart card evolution," *Communications of the Acm,* vol. 45, pp. 83-88, Jul 2002.

[18] M. Hendry, *Smart Card Security and Applications, 2nd ed.* Norwood, USA: Artech House, Inc., 2001.

[19] D. M'Raihi and M. T. Yung, "E-commerce applications of smart cards," *Computer Networks-the International Journal of Computer and Telecommunications Networking,* vol. 36, pp. 453-472, 2001.

[20] R. Anderson and M. Kuhn, "Tamper resistance: a cautionary note," presented at the Proceedings of the 2nd conference on Proceedings of the Second USENIX Workshop on Electronic Commerce - Volume 2, Oakland, California, 1996.

[21] R. Anderson and M. Kuhn, "Low cost attacks on tamper resistant devices Security Protocols." vol. 1361, B. Christianson*, et al.*, Eds., ed: Springer Berlin / Heidelberg, 1998, pp. 125-136.

[22] A. T. S. Chan, "Integrating smart card access to Web-based medical information systems," presented at the Proceedings of the 2003 ACM symposium on Applied computing, Melbourne, Florida, 2003.

[23] I. Tutanescu, E. Sofron, and M.Ali, "Security of internet-connected computer networks," *Int. J. Internet Technol. Secur. Syst.,* vol. 2, pp. 109-121, 2010.

[24] W. Rankl, "Overview about attacks on smart cards," *Information Security Technical Report,* vol. 8, pp. 67-84, 2003.

[25] C.-j. Wang, X. -m. Niu, and Y. Zhang, "Anonymity in PKI Environment," presented at the Proceedings of the Third International Conference on International Information Hiding and Multimedia Signal Processing (IIH-MSP 2007) - Volume 01, 2007.

[26] Smar Card Alliance. (2002). *Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identifications Systems* [Online]. Available: http://atmel.com/dyn/resources/prod_documents/Smart_Card_Biometric_paper%20May02.pdf

[27] W. Rankl and W. Effing, *Smart Card Handbook*. Chichester: Wiley, 2003.

[28] W. H. Yang and S. P. Shieh, "Password authentication schemes with smart cards," *Computers & Security,* vol. 18, pp. 727-733, 1999.

[29] H.-S. Kim,S.-W. Lee, and K. -Y. Yoo, "ID-based password authentication scheme using smart cards and fingerprints," *SIGOPS Oper. Syst. Rev.,* vol. 37, pp. 32-41, 2003.

[30] K.-F. Chen and S. Zhong, "Attacks on the (enhanced) Yang-Shieh authentication," *Computers & Security,* vol. 22, pp. 725-727, 2003.

[31] C.-K. Chan and L. M. Cheng, "Cryptanalysis of a Timestamp-Based Password Authentication Scheme," *Computers & Security,* vol. 21, pp. 74-76, 2001.

[32] W. Yingjie and L. Jianhua, "Security improvement on a timestamp-based password authentication scheme," *Consumer Electronics, IEEE Transactions on,* vol. 50, pp. 580-582, 2004.

[33] J. Liu, L. Fan, and J. Li, "Cryptanalysis and improvement on Yang-Shieh authentication schemes," presented at the Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services, Markham, Ontario, Canada, 2006.

[34] A. S. K. Pathan and H. Choong Seon, "An Improved Timestamp-Based Password Authentication Scheme Using Smart Cards," in *The 9th International Conference on Advanced Communication Technology*, 2007, pp. 804-809.

[35] H. Delfs and H. Knebl, *Introduction to cryptography: principles and applications*: Springer-Verlag New York, Inc., 2001.

[36] J. S. Coron, "What is cryptography?," *Security & Privacy, IEEE,* vol. 4, pp. 70-73, 2006.

[37] F. Piper, "Introduction to cryptology," *Information Security Technical Report,* vol. 2, pp. 10-13, 1997.

[38] K. Y. Lam, S. L. Chung, M. Gu, and J. G. Sun, "Security middleware for enhancing interoperability of Public Key infrastructure," *Computers & Security,* vol. 22, pp. 535-546, 2003.

[39] D. Coppersmith, C. Holloway, S. M. Matyas, and N. Zunic, "The data encryption standard," *Information Security Technical Report,* vol. 2, pp. 22-24, 1997.

[40] National Institute of standards and Technology. (2001). *Announcing the ADVANCED ENCRYPTION STANDARD (AES)* [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[41] X. Peng, P. Zhang, and L. Cai, "Information security system based on virtual-optics imaging methodology and public key infrastructure," *Optik - International Journal for Light and Electron Optics,* vol. 115, pp. 420-426, 2004.

[42] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the Acm,* vol. 21, pp. 120-126, 1978.

[43] R. Hunt, "Technological infrastructure for PKI and digital certification," *Computer Communications,* vol. 24, pp. 1460-1471, 2001.

[44] L. Kocarev and Z. Tasev, "Public-key encryption based on Chebyshev maps," in *ISCAS '03. Proceedings of the 2003 International Symposium on Circuits and Systems, 2003* , pp. III-28-III-31 vol.3.

[45] C.-K. Wu, "Hash channels," *Computers & Security,* vol. 24, pp. 653-661, 2005.

[46] M. J. Ganley, "Digital signatures," *Information Security Technical Report,* vol. 2, pp. 12-22, 1998.

[47] J. Weiss, "Message Digests, Message Authentication Codes, and Digital Signatures," in *Java Cryptography Extensions*, San Francisco: Morgan Kaufmann, 2004, pp. 101-118.

[48] D. M. Evans and D. C. Yen, "Private key infrastructure: balancing computer transmission privacy with changing technology and security demands," *Computer Standards & Interfaces,* vol. 27, pp. 423-437, 2005.

[49] E. G. Carayannis and E. Turner, "Innovation diffusion and technology acceptance: The case of PKI technology," *Technovation,* vol. 26, pp. 847-855, Jul 2006.

[50] C. K. Williams, "Configuring enterprise public key infrastructures to permit integrated deployment of signature, encryption and access control systems," *Military Communications Conference, 2005. MILCOM 2005, vols 1-5,* pp. 2172-2175.

[51] M. Spalding, "Deciding Whether or not to use a Third Party Certificate Authority," *Network Security,* vol. 2000, pp. 7-8, 2000.

[52] K. Viswanathan, C. Boyd, and E. Dawson, "Hybrid Key Escrow: A New Paradigm," *Computers & Security,* vol. 21, pp. 77-92, 2001.

[53] S. Lancaster, D. C. Yen, and S. -M. Huang, "Public key infrastructure: a micro and macro analysis," *Computer Standards & Interfaces,* vol. 25, pp. 437-446, 2003.

[54] R. Perlman, "An overview of PKI trust models," *Ieee Network,* vol. 13, pp. 38-43, Nov-Dec 1999.

[55] Corell and Simon, "Ten Risks of PKI: In Favour of Smart Card-Based PKI," *Network Security,* vol. 2000, pp. 12-14, 2000.

[56] T. E. Carroll and D. Grosu, "A secure and anonymous voter-controlled election scheme," *Journal of Network and Computer Applications,* vol. 32, pp. 599-606, 2009.

[57] M. Faundez-Zanuy, "Biometric security technology," *Ieee Aerospace and Electronic Systems Magazine,* vol. 21, pp. 15-26, 2006.

[58] D. D. Hwang and I. Verbauwhede, "Design of portable biometric authenticators energy, performance, and security tradeoffs," *Ieee Transactions on Consumer Electronics,* vol. 50, pp. 1222-1231, 2004.

[59] Y.-P. Li, "Biometric technology overview," *Nuclear Science and Techniques,* vol. 17, pp. 97-105, 2006.

[60] K. L. Kroeker, "Graphics and security: exploring visual biometrics," *Computer Graphics and Applications, IEEE,* vol. 22, pp. 16-21, 2002.

[61] M. Faundez-Zanuy, "On the vulnerability of biometric security systems," *Aerospace and Electronic Systems Magazine, IEEE,* vol. 19, pp. 3-8, 2004.

[62] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Communications of the Acm,* vol. 43, pp. 90-98, Feb 2000.

[63] J. Chirillo and S. Blaul, *Implementing Biometric Security*. New York: Wiley, 2003.

[64] B. Schouten and B. Jacobs, "Biometrics and their use in e-passports," *Image and Vision Computing,* vol. 27, pp. 305-312, 2009.

[65] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identity-authentication system using fingerprints," *Proceedings of the Ieee,* vol. 85, pp. 1365-1388, 1997.

[66] Y. Lin, X. Maozhi, and Z. Zhiming, "Digital signature systems based on smart card and fingerprint feature," *Journal of Systems Engineering and Electronics,* vol. 18, pp. 825-834, 2007.

[67] M. Crosbie, "Biometrics for enterprise security," *Network Security,* vol. 2005, pp. 4-8, 2005.

[68] V. Zorkadis and P. Donos, "On biometrics-based authentication and identification from a privacy-protection perspective - Deriving privacy-enhancing requirements.," *Information Management & Computer Security,* vol. 12, pp. 125-137, 2004.

[69] "Face recognition," *Biometric Technology Today,* vol. 16, pp. 9-11, 2008.

[70] N. Desmarais, "Body language, security and e-commerce," *Library Hi Tech,* vol. 18, pp. 61-74, 2000.

[71] C. Vivaracho-Pascual, M. Faundez-Zanuy, and J. M. Pascual, "An efficient low cost approach for on-line signature recognition based on length normalization and fractional distances," *Pattern Recognition,* vol. 42, pp. 183-193, 2009.

[72] A. J. Harris and D. C. Yen, "Biometric authentication: assuring access to information," *Information Management & Computer Security,* vol. 10, pp. 12 - 19, 2002.

[73] G. Duffield and P. Grabosky. (2001). *The Psychology of Fraud* [Online]. Available: http://www.aic.gov.au/publications/tandi/ti199.pdf

[74] P. S. Dowland, S. M. Furnell, H. M. Illingworth, and P. L. Reynolds, "Computer crime and abuse: A survey of public attitudes and awareness," *Computers & Security,* vol. 18, pp. 715-726, 1999.

[75] "Transit and Retail Payment: Opportunities for Collaboration and Convergence," Smart Card Alliance, Princeton Junction, NJ, Rep. PT-03005, 2003.

[76] H. N. Dreifus and J. T. Monk, *Smart cards: a guide to building and managing smart card applications*. Chichester: Wiley, 1998.

[77] ACI World Wide. (2007). *Smart Credit and Debit Payments* [Online]. Available: http://www.aciworldwide.com/pdfs/Smart_Credit_and_Debit_Pmts.pdf

[78] Federal Trade Commission. (2002). *Credit, ATM, and Debit Cards: What to do if they're lost or stolen?* [Online]. Available: http://www.ftc.gov/bcp/conline/pubs/credit/atmcard.pdf

[79] H. Leitold, A. Hollosi, and R. Posch, "Security Architecture of the Austrian Citizen Card Concept," in *Proceedings of the 18th Annual Computer Security Applications Conference*, 2002, pp. 391-400.

[80] Central Informatics Organization. (2006). *Smart Card Uses and Benefits* [Online]. Available: http://www.smartcard.gov.bh/index.php?module=ContentExpress&func=display&ceid=33

[81] C. Lambrinoudakis, S. Gritazalis, F. Dridi, and G. Pernul, "Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy," *Computer Communications,* vol. 26, pp. 1873-1883, 2003.

[82] "UK's national ID card procurement begins," *Card Technology Today,* vol. 19, pp. 3-4, 2007.

[83] H. Kwok and N. Stevens, "Dynamic patient data bases: the foundation of an integrated approach to outcome measures for the healthcare professionals," *Medinfo,* vol. 8, p. 483, 1995.

[84] R. Zielstorff, "Capturing and using clinical outcome data: implications for information systems design," *Journal of the American Medical Informatics Association,* vol. 2, pp. 191-196, 1995.

[85] C. T. Liu, P. T. Yang, Y. T. Yeh, and B. L. Wang, "The impacts of smart cards on hospital information systems--An investigation of the first phase

of the national health insurance smart card project in Taiwan," *International Journal of Medical Informatics,* vol. 75, pp. 173-181, 2006.

[86] CardWrek. (2008). *Loyalty Card Solutions, Smart Membership and Gift Cards* [Online]. Available: http://www.cardwerk.com/smart-card-solutions/loyalty-card/

[87] N. T. M. Demoulin and P. Zidda, "On the impact of loyalty cards on store loyalty: Does the customers' satisfaction with the reward scheme matter?," *Journal of Retailing and Consumer Services,* vol. 15, pp. 386-398, 2008.

[88] C. Mauri, "Card loyalty. A new emerging issue in grocery retailing," *Journal of Retailing and Consumer Services,* vol. 10, pp. 13-25, 2003.

[89] Boots. (2008). *Advantage Card application* [Online]. Available: https://www.boots.com/adcard/index.jsp?fromPage=apply&fromHoldingPage=yes&registered=no&adCardNum=

[90] Review Centre. (2008). *Boots advantage card reviews* [Online]. Available: http://www.reviewcentre.com/reviews7277.html

[91] P. T. Blythe, "Improving public transport ticketing through smart cards," *Proceedings of the Institution of Civil Engineers-Municipal Engineer,* vol. 157, pp. 47-54, Mar 2004.

[92] M. Bagchi and P. R. White, "The potential of public transport smart card data," *Transport Policy,* vol. 12, pp. 464-474, 2005.

[93] S. Konomi and G. Roussos, "Ubiquitous computing in the real world: lessons learnt from large scale RFID deployments," *Personal and Ubiquitous Computing,* vol. 11, pp. 507-521, Oct 2007.

[94] "London's Oyster card goes public," *Card Technology Today,* vol. 15, pp. 1-1, 2003.

[95] "New sQuid on the e-purse block," *Card Technology Today,* vol. 18, pp. 1-1, 2006.

[96] H. Bryan and P. Blythe, "Understanding behaviour through smartcard data analysis," *Proceedings of the Institution of Civil Engineers-Transport,* vol. 160, pp. 173-177, Nov 2007.

[97] J. Slay and A. Koronios, *Information technology security and risk management*. Queensland Australia: John Wiley, 2006.

[98] R. Weber, *Information System Control and Audit*, 6th ed. Great Britain: Prentice Hall, 1998.

[99] D. Gollmann, *Computer Security*, 2nd ed. Chichester: John Wiley, 2006.

[100] K. Markantonakis, M. Tunstall, G. Hancke, L. Askoxylakis, and K. Mayes, "Attacking smart card systems: Theory and practice," *Information Security Technical Report,* vol. 14, pp. 46-56, 2009.

[101] X. Leng, "Smart card applications and security," *Information Security Technical Report,* vol. 14, pp. 36-45, 2009.

[102] K. Nohl, D. Evans, S. Starbug, and P. Henryk, "Reverse-engineering a cryptographic RFID tag," *presented at the Proceedings of the 17th conference on Security symposium*, San Jose, CA, 2008, pp. 185-193.

[103] T. Boswell, "Smart card security evaluation: Community solutions to intractable problems," *Information Security Technical Report,* vol. 14, pp. 57-69, 2009.

[104] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," in *Cryptographic Hardware and Embedded Systems - CHES 2004*, ed, 2004, pp. 135-152.

[105] P. C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," *presented at the Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, 1999, pp. 388-397.

[106] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan, "The Sorcerer's Apprentice Guide to Fault Attacks," *Proceedings of the Ieee,* vol. 94, pp. 370-382, 2006.

[107] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal,* vol. 40, pp. 614-634, 2001.

[108] C. Roberts, "Biometric attack vectors and defences," *Computers & Security,* vol. 26, pp. 14-25, 2007.

[109] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An Analysis of Minutiae Matching Strength," *presented at the Proceedings of the Third International Conference on Audio- and Video-Based Biometric Person Authentication*, 2001, pp. 223-228.

[110] B. Cukic and N. Bartlow, "The vulnerabilities of biometric systems - An integrated look and old and new ideas," *Technical Report,* 2005.

[111] F. Sabena, A. Dehghantanha, and A. P. Seddon, "A Review of Vulnerabilities in Identity Management Using Biometrics," in *ICFN '10. Second International Conference on Future Networks*, 2010, pp. 42-49.

[112] M. Martinez-Diaz, J. Fierrez-Aguilar, F. Alonso-Fernandez, J. Ortega-Garcia, and J. A. Siguenza, "Hill-Climbing and Brute-Force Attacks on Biometric Systems: A Case Study in Match-on-Card Fingerprint Verification," in *Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International*, 2006, pp. 151-159.

[113] J. L. Wayman, "Technical Testing and Evaluation of Biometric Identification Devices," in *Biometrics*, A. K. Jain, *et al.*, Eds., ed: Springer US, 2002, pp. 345-368.

[114] N. Ferguson and B. Schneier, *Practical Cryptography*, 1st ed. Indiana: John Wiley, 2003.

[115] A. Kaliontzoglou, P. Sklavos, T. Karantjias, and D. Polemi, "A secure e-Government platform architecture for small to medium sized public organizations," *Electronic Commerce Research and Applications,* vol. 4, pp. 174-186, 2005.

[116] M. Fouad, Private Communication, April 2008.

[117] F. den Braber, I. Hogganvik, M. S. Lund, K. Stolen, and F. Vraalsen, "Model-based security analysis in seven steps - a guided tour to the CORAS method," *Bt Technology Journal,* vol. 25, pp. 101-117, Jan 2007.

[118] I. Hogganvik and K. Stolen, "Risk analysis terminology for IT-systems: Does it match intuition?," *2005 International Symposium on Empirical Software Engineering (Isese), Proceedings,* 2005, pp. 13-22.

[119] ioMosaic Corporation. (2002). *Designing an Effective Risk Matrix* [Online]. Available: http://archives1.iomosaic.com/whitepapers/risk-ranking.pdf

[120] APACS the UK Payements Administrations. (2008). *Fraud figures announced by APACS*. Available: http://www.ukpayments.org.uk/media_centre/press_releases/-/page/685/

[121] Smart Card Alliance. (2010). *Medical Identity Theft in Healthcare* [Online]. Available: http://www.smartcardalliance.org/pages/publications-medical-identity-theft-in-healthcare

[122] E. Nafea, Private Communication, March 2008.

[123] Anonymous, Private Communication, May 2008.

[124] T. R. Peltier, *Information Security Risk Analysis*, 2nd ed. Auerbach: CRC Press LLC, 2001.

[125] Smart Card Alliance. (2009). *A Healthcare CFO's Guide to Smart Card Technology and Applications* [Online]. Avaiable: http://www.smartcardalliance.org/pages/publications-healthcare-guide-smart-card-technology-applications

[126] O. Wyman. (2008). *PULSE 2008 Debit Issuer Study Reveals Continued Debit Growth and Potential for Improved Performance Among U.S. Debit Card Issuer* [Online]. Available: http://www.remittancedirectory.com/pdfReader.jsp?document=/docs/PULSE050208.pdf

[127] Smart Card Alliance. (2009). *Fraud in the U.S. Payments Industry: Chip Card Technology Impact on Fraud* [Online]. Available: http://www.smartcardalliance.org/pages/publications-fraud-in-the-us-payments-industry

[128] J. Spertus. (2003). *Operation Decrypt Leads to Charges Against 17 For Developing Technology Used to Steal Millions of Dollars Worth of Satellite TV Six Defendants Charged Under Digital Millennium Copyright Act* [Online]. Available: http://www.justice.gov/criminal/cybercrime/OPdecrypt_walterPlea.htm

[129] H. Graupner. (2010). *Concerns raised over security of new German ID cards* [Online]. Available: http://www.dw-world.de/dw/article/0,,5945076,00.html

[130] V. Helmbreck. (2008). *Smartcard hacking trick* [Online]. Available: http://www.financetechnews.com/smartcard-hacking-trick/

[131] Datamonitor. (2004). *The ROI case for smart cards in the enterprise* [Online]. Available: http://mediaforms.siemensenterprisemedia.com/forms/_docs/Smart%20cards%20ROI%20white%20paper.pdf

[132] P. R. Garvey and Z. F. Lansdowne, "Risk Matrix: An Approach for Identifying, Assessing, and Ranking Program Risk," *Air Force journal of logistics,* vol. 22, pp. 18-21, 1998.

[133] S. Schneider, “Security properties and CSP,” in *Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on,* 6-8 1996, pp. 174 –187.

[134] J. McDermott, "Visual security protocol modeling," *presented at the Proceedings of the 2005 workshop on New security paradigms*, Lake Arrowhead, California, 2005.

[135] Object Management Group. (2005). *Introduction to OMG's Unified Modeling Language* [Online]. Available: http://www.omg.org/gettingstarted/what_is_uml.htm

[136] J. Jürjens, "Modelling audit security for Smart-Card payment schemes with UML-SEC," *presented at the Proceedings of the 16th international conference on Information security: Trusted information: the new decade challenge*, Paris, France, 2001.

[137] J. Jürjens, "UMLsec: Extending UML for Secure Systems Development," in *«UML» 2002 — The Unified Modeling Language*, ed, 2002, pp. 1-9.

[138] J. Jürjens, "Using UMLsec and goal trees for secure systems development," *presented at the Proceedings of the 2002 ACM symposium on Applied computing*, Madrid, Spain, 2002.

[139] J. Jürjens, J. Schreck, and Y. Yu, "Automated analysis of permission-based security using UMLsec," *presented at the Proceedings of the Theory and practice of software, 11th international conference on Fundamental approaches to software engineering*, Budapest, Hungary, 2008.

[140] D. Everett. (2008). *Mifare Chip Hacked Again - Oh Dear!* [Online]. Available: http://www.smartcard.co.uk/members/newsletters/2008/SCN%20March%202008.pdf

[141] J. Xu, W. -T. Zhu, and D. -G. Feng, "An improved smart card based password authentication scheme with provable security," *Computer Standards & Interfaces,* vol. 31, pp. 723-728, 2009.

[142] D. Moon, Y. Chung, S. B. Pan, and J. -W. Park, "Integrating fingerprint verification into the smart card-based healthcare information system," *EURASIP J. Adv. Signal Process,* vol. 2009, pp. 5-5, 2009.

[143] P. Beynon-Davies, "Personal identity management and electronic government: The case of the national identity card in the UK," *Journal of Enterprise Information Management,* vol. 20, 2007.

[144] P. Ezudheen, P. Chandran, J. Chandra, B. P. Simon, and D. Ravi, "Parallelizing SystemC Kernel for Fast Hardware Simulation on SMP Machines," in *Pads 2009: 23rd Workshop on Principles of Advanced and Distributed Simulation, Proceedings*, ed Los Alamitos: Ieee Computer Soc, 2009, pp. 80-87.

[145] K. Rothbart, U. Neffe, Ch. Steger, R. Weiss, E. Rieger, and A. Muehlberger, "Extended abstract: an environment for design verification of smart card systems using attack simulation in SystemC," in *Formal Methods and Models for Co-Design, 2005. MEMOCODE '05. Proceedings. Third ACM and IEEE International Conference on*, 2005, pp. 253-254.

[146] Open SystemC Initiative. (2010). *About SystemC* [Online]. Available: http://www.systemc.org/community/about_systemc/

[147] P. R. Panda, "SystemC - a modeling platform supporting multiple design abstractions," in *System Synthesis, 2001. Proceedings. The 14th International Symposium on*, 2001, pp. 75-80.

[148] D. Black and J. Donovan, *SystemC: From The Ground Up*, 1st ed. USA: Springer, 2004.

[149] L. Chen, W. -Z. Sun, Z. -X. Wang, and C. Zhou, "A SystemC-Based Transaction Level Modeling of On-Chip-Bus," in *Computer Science and Software Engineering, 2008 International Conference on*, 2008, pp. 146-149.

[150] V. Galiano, M. Martinez, H. Migallon, D. Perez-Caparros, and C. Quesada, "A case study in distributing a SystemC model," in *Distributed Computing, Artificial Intelligence, Bioinformatics, Soft Computing, and Ambient Assisted Living. 10th International Work-Conference on Artificial Neural Networks, IWANN 2009 Workshops*, Salamanca, Spain, 2009, pp. 99-106.

[151] K. Rothbart, U. Neffe, Ch. Steger, R. Weiss, E. Rieger, and A. Muehlberger,, "High level fault injection for attack simulation in smart cards," in *Test Symposium, 2004. 13th Asian*, 2004, pp. 118-121.

[152] "IEEE Standard System C Language Reference Manual," *IEEE Std 1666-2005,* pp. 0_1-423, 2006.

[153] L. Cai and D. Gajski, "Transaction level modeling: an overview," *presented at the Proceedings of the 1st IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis,* Newport Beach, CA, USA, 2003.

[154] C. Helmstetter, F. Maraninchi, and L. Maillet-Contoz, "Full simulation coverage for SystemC transaction-level models of systems-on-a-chip," *Formal Methods in System Design,* vol. 35, pp. 152-189, Oct 2009.

[155] J. Aynsley, "OSCI TLM-2.0 LANGUAGE REFERENCE MANUAL," Open SystemC Initiative, 2009.

[156] N. Bombieri, F. Fummi, and V. Guarnieri, "Automatic synthesis of OSCI TLM-2.0 models into RTL bus-based IPs," in *High Level Design Validation and Test Workshop (HLDVT), 2010 IEEE International*, 2010, pp. 105-112.

[157] S. Pasricha, "Transaction level modeling of SoC with SystemC 2.0," *presented at the Synopsys User Group Conference*, 2002.

[158] P. Pierre. (2002). StepNP: A System-Level Exploration Platform for Network Processors. pp. 17-26. Available: http://doi.ieeecomputersociety.org/10.1109/MDT.2002.1047740

[159] C.-Y. Yang, C. -C. Lee, and S. -Y Hsiao , "Man-in-the-middle attack on the authentication of the user from the remote autonomous object," *International Journal of Network Security,* vol. 1, pp. 81–83, 2005.

[160] J. Alves-Foss, "Multi-Protocol Attacks and the Public Key Infrastructure," in *In Proc. National Information System Security Conference*, Arlington, 1998, pp. 566-576.

[161] A. M. Johnston and P. S. Gemmell, "Authenticated Key Exchange Provably Secure Against the Man-in-the-Middle Attack," *Journal of Cryptology,* vol. 15, pp. 139-148, 2002.

Appendix A

Information Security Risk Analysis Tables

	Time Sensitivity	**Intangible Loss** (dollar loss difficult to estimate)			**Tangible Loss**
Impact Value	**Longest Tolerable Outage Period during Peak**	**Health and Safety**	**Customer Satisfaction (dissatisfied customers)**	**Embarrassment (comes to the attention of)**	**Financial**
Very High	24 hours or Less	Loss of multiple lives	More than 500,000	National or International • Press • Organisation	More than $10M
High	25-72 hours	Loss of life	100,001 - 500K	Local or State • Press • Organisation	$1,000,001 - $10M
Medium	73 hours-5days	Serious injury	10,001 - 100K	Company Organisation	$100,001 – 1M
Low	6-9 days	Major exposure to unsafe work environment	1001 – 10K	Company Division	$50,001 - $100K
Very Low	10 days or more	Little or no negative impact	0 – 1K	Few if anyone or company group	$0 - $50K

Table (A.19): Loss Impact Table
Source: [124]

Impact Value	Information Classification	Longest Tolerable Outage
Very High	**Top Secret-** Information that, if disclosed, could cause severe impact to the company's competitive advantage or business strategies	24 hours or less
High	**Confidential-** Information that, if disclosed, could violate the privacy of individuals, reduce competitive advantage, or damage the company	25-72 hours
Medium	**Restricted-** Information that is available to a specific subset of the employee population when conducting company business	73 hours-5 days
Low	**Internal use-** Information that is intended for use by all employees when conducting business	6-9 days
Very Low	**Public-** Information that has been made available to the public through authorised company channels	10 days or more

Table (A.20): Information Classification Table
Source: [124]

Appendix B

Publications

The following paper is published during the course of this thesis work:

A. Bushager and M. Zwolinski, "Modelling Smart Card Security Protocols in SystemC TLM," in *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*, 2010, pp. 637-643.

Modelling Smart Card Security Protocols in SystemC TLM

Aisha Bushager and Mark Zwolinski
School of Electronics and Computer Science
University of Southampton
Southampton SO17 1BJ, UK
Email:{afb05r,mz}@ecs.soton.ac.uk

***Abstract*—Smart cards are an example of advanced chip technology. They allow information transfer between the card holder and the system over secure networks, but they contain sensitive data related to both the card holder and the system, that has to be kept private and confidential. The objective of this work is to create an executable model of a smart card system, including the security protocols and transactions, and to examine the strengths and determine the weaknesses by running tests on the model. The security objectives have to be considered during the early stages of systems development and design; an executable model will give the designer the advantage of exploring the vulnerabilities early, and therefore enhancing the system security. The Unified Modeling Language (UML) 2.0 is used to model the smart card security protocol. The executable model is programmed in SystemC with the Transaction Level Modeling (TLM) extensions. The final model was used to examine the effectiveness of a number of authentication mechanisms with different probabilities of failure. In addition, a number of probable attacks on the current security protocol were modeled to examine the vulnerabilities. The executable model shows that the smart card system security protocols and transactions need further improvement to withstand different types of security attacks.**

I. Introduction

In our digital era, smart cards are a central piece of the wireless revolution. They have entered our wallets as a highly secure key to services that are essential to our daily interaction with the digital world. A smart card allows information transfer between the card holder and a system over secure networks; it contains sensitive data related to both the card holder and the system that has to be kept private and confidential. Therefore, security has to be considered as a key requirement during the early stages of systems development.

The objective of this work is to create an executable model of a smart card system, including the security protocols and transactions, to allow examination of the strengths and weaknesses by executing tests on the model.

The Unified Modelling Language (UML) version 2.0 has been widely used to model smart card security protocols. For example, UMLsec [1] is an extension to UML for integrating security related information into UML specifications by specifying security requirements through stereotypes, tagged values, and constraints.

On the other hand, the models produced by UML are static. In this work we have developed executable models in SystemC, which is a set of C++ classes that provide an event-driven simulation kernel. SystemC is a system level modelling language; it enables design and verification at the system level, independent of any detailed hardware and software implementation. On top of SystemC, Transaction Level Modelling (TLM) is used to model the transactions of the smart card system.

II. Related Work

Security protocols are sets of rules designed to ensure particular security goals. However, designing and implementing these protocols is difficult and they may fail against various attacks. To be able to effectively integrate the security protocols at early development stages, modelling languages and techniques are used to better visualise the entire system. One such modelling tool is Communicating Sequential Processes (CSP), which is a process algebra that is used to describe and analyse security properties and protocols by providing a mathematical framework [2]. However, to be able to use CSP, the designer must have specialised knowledge and training, which limits the usage of this method. GSPML, [3], is a visual security protocol modelling language. Again, this language introduces notations and complex models that are targeted to security specialists.

UML can model both the static structure and the dynamic behaviour of the system [4]. To support UML for secure systems development, an extension called UMLsec has been proposed, [1], [5]. UMLsec uses a combination of use-case driven processes with a goal directed approach. The three main mechanisms of the extension are stereotypes, tags, and constraints [6]. Stereotypes and tags are used to create and present the security requirements and assumptions, constraints may be attached but they should be satisfied by modelling elements with the related stereotype [5]. An adversary can be created in UMLsec to model possible threats to a system. UMLsec was used to find possible vulnerabilities in Common Electronic Purse Specifications (CEPS) [1], it was also used to define security permissions that enforce restrictions on the workflows of a system [7].

None of the above modelling languages provides an automatic transition from design to code implementation. A designer would like to have an executable model that allows a better testing of the designed model and therefore links the gap between the design phase and the code implantation

phase. In our work, an executable model is produced using SystemC with the TLM extensions [8]. SystemC has been used to produce a methodology to simulate security attacks on smart cards with fault injection [9] and it has also been used to create an environment for design verification of smart cards using security attack simulation [10]. In TLM, communication among computation components is modelled by channels and transaction requests go on by calling interface functions of these channel models [11].

III. Smart Card System Security

Because the smart cards are used to store sensitive data such as PINs, passwords, and keys; the main purpose of an attack is to get hold of these data. Attackers might perform various numbers and styles of attacks on the smart card system.

A. Smart Card System Threats

Threats are the possible means by which a security policy may be breached [12]. A threat source can be any person, thing, event, or idea that poses danger to an asset within a system in terms of confidentiality, integrity, availability, or legitimate use. Moreover, threats can be deliberate or accidental [12]. If deliberate, a threat can be categorised as passive, such as network sniffing, or active, such as negligence, errors, attempt to gain unauthorised access to the system, or changing the value of a particular transaction by malicious persons. Therefore, possible threats on the smart card system include unauthorised system access, hacking and system intrusion, information leakage or theft, integrity violation (errors and omissions by insiders or outsiders), distributed denial of service, illegitimate use (dishonest or disgruntled insiders or outsiders), system penetration and tampering. Threat sources have different motivations that may lead to carrying out various attacks on any government or business information system; therefore, the parties involved in the smart card system must be familiar with the human threat environments and their different motivations.

B. Possible Attacks on a Smart Card System

Security is a huge matter; it covers every single stage of a products lifecycle, starting from the development stage, the manufacturing stage, and ending up with actual usage. Attacks that take place at the development stage and the manufacturing stage of a smart card are most likely carried out by an insider, [13] . Attacks during the smart card use stage can be physical or logical [13]. Physical attacks may manipulate the semiconductor itself and usually require equipment like microscopes, focused ion beams, etc. [14]. Side-channel attacks consist of observing behaviour while the information is being processed and include timing analysis and power analysis [15].

In contrast, logical attacks or so called software attacks do not attack the hardware properties directly; they are more focused on the communication and flow of information between the smart card and the terminal [13]. Attackers can write malicious software, that can be employed in a software attack on a smart card, for example, in smart cards that support Java Card it is possible to load and run software. Examples of logical attacks could be bug exploits, illegal bytecode, and attacks during PIN comparison.

Other types of attacks take place during the authentication phase of the smart card system, where the user identity is authenticated using different types of authentication mechanisms like biometrics [16].

IV. Using UML to Model Smart Card Transactions

A robust and secure smart card system requires an optimal selection of policies, procedures, protocols, architecture, technology, and staff. To have a better idea of the smart card system and its components, operations, applications, data and information, and security mechanisms, we use a number of UML diagrams for illustration.

A. Overview of a Smart Card System

Figure 1 is a use case diagram that gives an overview of the basic components and functions of any smart card system. The use case diagram is a behavioural UML diagram that presents the system functionality. In our system, the actors illustrated in the figure represent the main components of the system, which are the User, Smart Card, Smart Card Reader, Client, Server, and Database. The use cases represent the functions or services that take place while the system is operating. The focus of the analysis in this study will be on the functions of three main components, which are the User, Smart Card, and the Smart Card Reader.

When the User decides to use the Smart Card, the first step is to insert the Smart Card in the Smart Card Reader. The Smart Card Reader has number of jobs: it has to verify and authenticate the User and Smart Card, commit transactions, and exchange and confirm the User details with the other system components. To be able to demonstrate the transactions of the system, another type of UML diagram has to be used. The following sections describe the registration phase and the verification phase of the smart card system.

B. Smart Card Registration System

To be able to demonstrate the transactions and message sequence between the smart card system objects, a sequence diagram is used; it is a behavioural diagram that shows the interactions of system processes.

Figure 2 shows the enrolment process that is the main part of the Registration System. The model uses a combination of PINs and biometrics to enhance the verification process. In addition, the Public Key Infrastructure (PKI) is employed to fulfil the system security requirements. PKI is considered to be one of the most comprehensive and secure schemes of passing information from one point to the other. It uses a trusted third party for implementing key life-cycle management processes. This third party is called the Certificate Authority (CA), which validates the identity of the user and issues digital certificates [17].

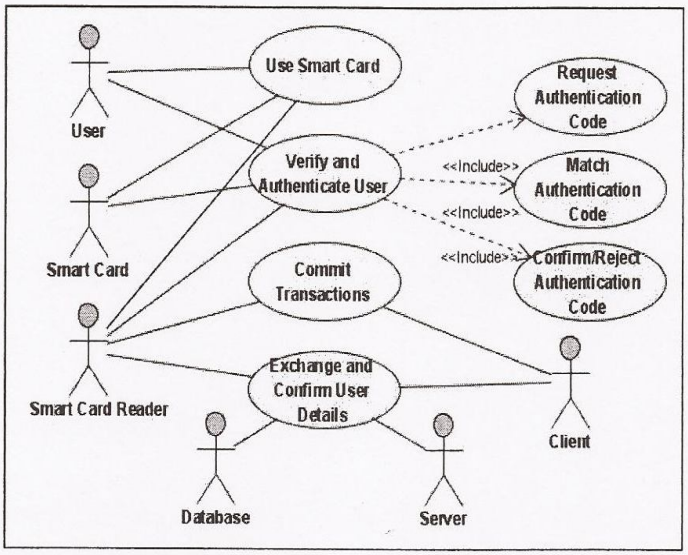

Fig. 1. Overview of a Smart Card System.

The User provides the required information along with the biometric evidence. The system then saves the User details in the Smart Card and captures the fingerprint, which is the biometric method used in the proposed design, and produces a template that is stored in the system and the Smart Card. Then, the Registration System requests a PIN from the User to be used in future verification processes.

The PIN is stored in the Smart Card for future verification. Finally, the smart card system requests a private key from the CA to generate a digital signature. The CA, on the other hand, requests User verification from the Registration System, generates a pair of keys for the User. The CA also issues a digital certificate corresponding to the public key, and sends the private key to the Smart Card to generate a digital signature that combines the private key and the biometric template of the User.

C. Smart Card System Verification

Figure 3 shows the transactions that take place when the User uses the Smart Card in a security environment that combines PIN, Biometrics, and PKI security methods.

The User first inserts the PIN, the Smart Card Reader extracts the stored PIN from the Smart Card and starts the comparison process. If the match is successful the Smart Card Reader will ask for another proof, which is the Users fingerprint, otherwise, the transaction will be aborted after allowing the User three attempts to enter the PIN. The User scans the finger through the Smart Card Reader scanner; the Reader will extract the User's biometric feature and produce a template. The matching process will then take place and the result will decide whether the User has the permission to access the system or not. If the match was true, the Smart Card releases the User's private key. Next, the User starts to send a message to the Receiver; the message is going to be digitally signed with the User's private key, and the system will request the Receiver's public key from the CA to encrypt the message. The CA will send the digital certificate and the message will be encrypted using both the User's private key and the Receiver's pubic key, therefore, the digital envelope is now ready to be sent securely to the Receiver. Finally, the Receiver will send a request to the CA to get the Sender's public key to decrypt the message. Again, using both the Sender's public key and the Receiver's private key the Receiver will be able to decrypt the message successfully.

These security methods should achieve the security goals of confidentiality, integrity, authentication, and non-repudiation. However, each mechanism has its pros and cons, the possible attacks that might take place are shown in Figure 3. For example, fingerprints have disadvantages: How can we know that the biometric provided is not subject to misuse? If the User was clever and powerful enough to fool the system and use a false fingerprint, then the system will be breached and an intruder will have access to the real User's credentials and privileges. The PKI method has its disadvantages as well. If one breach takes place during the transaction the Sender and the Receiver can both suffer security loss.

D. Modelling Attacks Using UMLsec

After using UML diagrams to express the smart card system protocol and processes, and to represent the transactions that take place while messages are exchanged during the registration and verification processes, in addition to knowing where are the areas that could be vulnerable to attacks, it is also essential to test the model against possible attacks. UMLsec was used to model attacks, using stereotypes such as *secrecy* and *secure information flow* along with their tags and constraints. An adversary type in UMLsec can have a function called *Threat* that allows the adversary to commit delete, read,

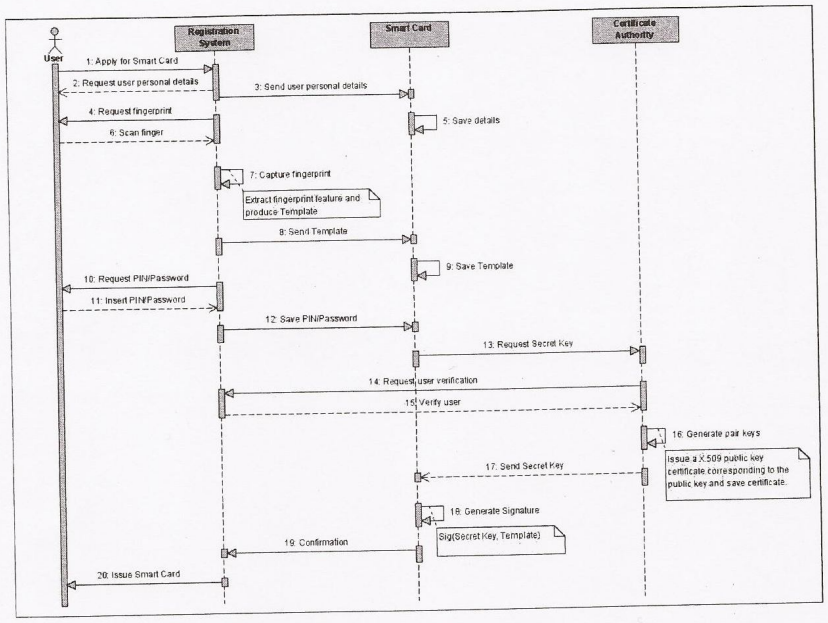

Fig. 2. Registration Phase in PIN, Biometrics (Fingerprint), and PKI Smart Card System.

and insert attacks. Even by writing these notations down, the model is still static and not executable.

As a result, UMLsec did not automate the model because it is a specification language that has the ability of expressing the system protocols and transactions but not automating them. Therefore, SystemC TLM was used to transform the static model into an executable model.

V. Animating the Model Using SystemC TLM

The SystemC library provides concurrent and hierarchical modules, ports, channels, processes, and clocks. Large designs are always broken down hierarchically to be able to manage complexity, structural decomposition of the simulated model in SystemC is specified with modules. The module is the smallest container with state, behaviour, and structure for hierarchical connectivity, the construct SC_MODULE is used to represent a module [8]. In our work, SC_THREAD is used – a thread process is associated with its own thread of execution. Once the thread starts executing it is in complete control of the simulation until it chooses to return control to the simulator. Hence, the thread process is used to model sequential behaviour [8]. SystemC has two ways to pass control to the simulator again, one way is to exit by (return), in this case the thread is totally stopped, the other way is by having a (wait), therefore, every thread contains an infinite loop and usually has at least one wait function.

In our model, the smart card system objects are programmed as SystemC modules, and the transactions among these modules are modelled using TLM. In TLM, transactions are implemented by function calls.

A. Smart Card System Simulation

The executable model produced in our work shows the sequence of transactions that occur in the smart card system while the smart card is used; they correspond to the transactions in Figure 3. The following is part of the simulation output produced:

```
sender_object://///////////////////////
sender_object:// Card count: 100
sender_object:// Card ID: 611
sender_object:// Pin entered: correct
sender_object:// entry duration: 1 s
sender_object://///////////////////////
sender_object: begin transition 1
smartcard_reader_object: begin transition 2
smartcard_reader_object: end transition 2
smartcard_reader_object: begin transition 3
```

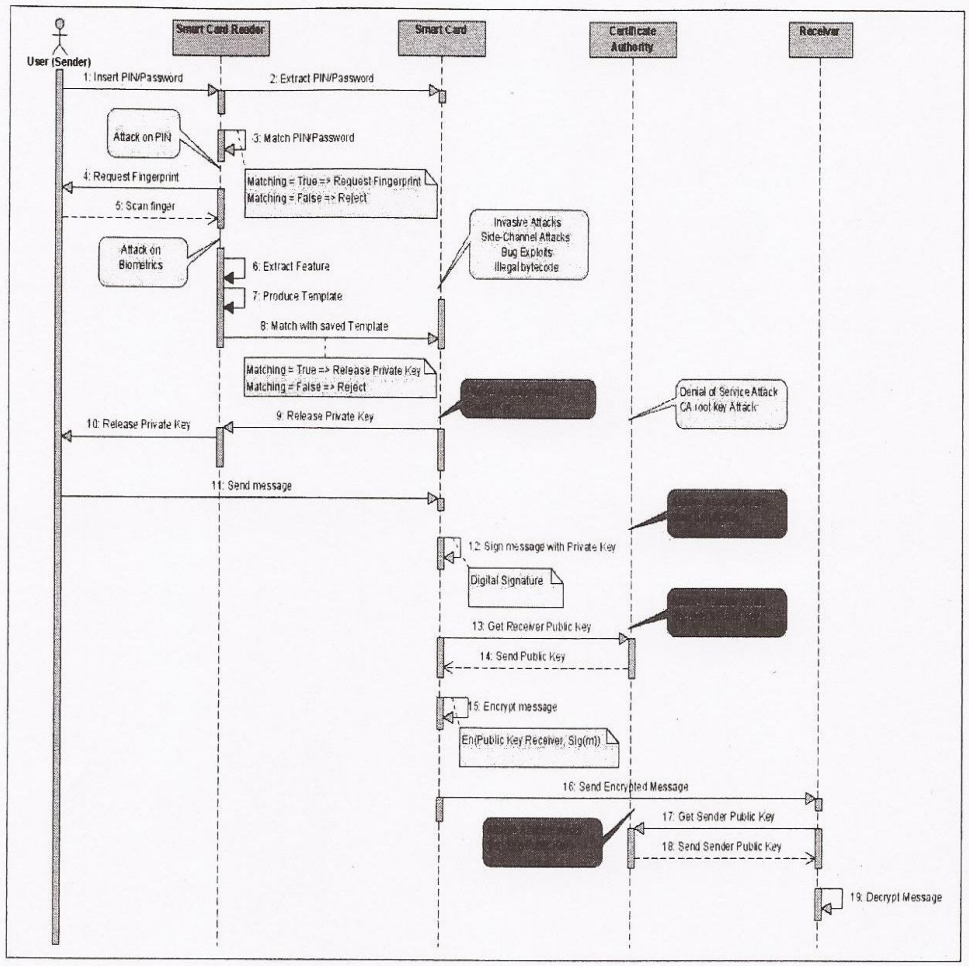

Fig. 3. Verification Processes in PIN, Biometrics (Fingerprint), and PKI Smart Card System.

```
smartcard_reader_object: Good pin
smartcard_reader_object: end transition 3
sender_object: end transition 1
sender_object: *** good pin decoded ***
smartcard_reader_object: begin transition 4
smartcard_reader_object: end transition 4
sender_object://////////////////////////
sender_object:// Card count: 100
sender_object:// Card ID: 611
sender_object:// Fingerprint entered: correct
sender_object:// Entry duration: 5 s
sender_object://////////////////////////
sender_object: begin transition 5
smartcard_reader_object: begin transition 6
smartcard_reader_object: end transition 6
smartcard_reader_object: begin transition 7
smartcard_reader_object: end transition 7
smartcard_reader_object: begin transition 8
smartcard_reader_object: end transition 8
sender_object: end transition 5
smartcard_object: begin transition 9
smartcard_reader_object: begin transition 10
smartcard_reader_object: end transition 10
smartcard_object: end transition 9
sender_object: begin transition 11
sender_object: end transition 11
smartcard_object: begin transition 12
smartcard_object: end transition 12
smartcard_object: begin transition 13
smartcard_object: end transition 13
cert_authority_object: begin transition 14
cert_authority_object: end transition 14
smartcard_object: begin transition 15
smartcard_object: end transition 15
smartcard_object: begin transition 16
smartcard_object: end transition 16
receiver_object: begin transition 17
receiver_object: end transition 17
cert_authority_object: begin transition 18
cert_authority_object: end transition 18
receiver_object: begin transition 19
receiver_object: end transition 19
```

The executable module shows the smart card system objects and their related transactions. The lifelines in the UML diagram are represented as objects, called modules in SystemC, and the arrows are represented as transactions using TLM. The

transitions in the output correspond to the transaction number in the UML diagram. Obviously, the designer can observe the attempts to enter the right PIN and Biometric along with the required timing. This allows the testing of the effectiveness of the authentication methods used. By running the simulation on different numbers of smart cards with different probabilities of failure it is possible to evaluate the effectiveness of each authentication method.

B. Simulating Attacks on Smart Card System

The executable model allows us to simulate an attack on the system. An attack on any part of the system is essentially another transaction inserted into the model. For example, to simulate an attack that allows the attacker to steal the private key released from the smart card object, which is coded as a state machine, an attacker is implemented as a class that can intrude into multiple modules in a thread-safe manner. Thus, a transaction is effectively inserted into the model by inserting the following line of code at the appropriate point in the smart card module:

```
attack::
getInstance().set_private_key(private_key);
```

Now, the model waits for transitions 1 to 8 to occur, and then the attacker interferes and attacks the system after transition 8 where the private key is released.

```
smartcard_reader_object: begin transition 8
smartcard_reader_object: end transition 8
sender_object: end transition 5
Attacker initialized, @104 s
Attacker stole the private key, @104 s
smartcard_object: begin transition 9
smartcard_object: end transition 9
```

The simulation shows that the attacker gets hold of the private key by practising a successful attack on the smart card object. Attacking the key exchange operation violates the privacy, authentication, and integrity properties of the system. Also, it compromises the security of the User, which may result in identity theft, information leackage, or message alteration. Being able to steal the private key points out a vulnerability within the security protocol employed in the system.

A Denial of Service (DOS) attack is simulated using the same model. The attack aims at violating the availability property of the system security. The DOS attack will take place against the Certificate Authority server; the attacker attempts to exhaust the server, which will result in the server being unable to provide the services for legitimate users. The following is part of the DOS attack simulation output:

```
iteration: 4 at time: 2 s 194
insert_pin_password 201
extract_pin_password 294
request_fingerprint 305
match_with_saved_templates 324
release_private_key 428
release_private_key 335
send message 217
get_receiver_public_key 438
send_encrypted_message 451
Attacker stole the sender public key,
SERVICE DENIED, @2 s 561
```

As the output shows, the transactions of the smart card system are running normally, however, when the DOS attack successfully takes place, the service is denied and the attacker gets hold of the users public keys exchanged among the system objects. In addition, the subsequent transactions failed to occur because the Certificate Authority server is unavailable. This attack shows that the availability property has been violated and the system users will not be able to use their smart cards until the Certificate Authority server recovers from the attack.

In summary, the executable model developed using SystemC TLM allowed the designer to discover the weak points of the system, the successful attacks indicate that there are weaknesses in the security protocol. A number of security properties like authentication, privacy, integrity, and availability have been violated, which shows that the system is vulnerable to attacks. To be able to reduce the probability of successful attacks, the designer can modify the executable model to test against future attacks.

In contrast with the UML diagram, the animation makes it possible to see the attack actually happening. Moreover, it is possible to make changes easily within the model and to try a number of attacks to test the system's robustness by simply inserting transactions into the UML diagram, and transforming them into transactions within the SystemC TLM executable model.

VI. Conclusion

UML diagrams are an excellent way of modelling systems, along with their extensions; they have features that show the designer how things should work. However, UML does not allow the designer to see what happens if something goes wrong with the system. Therefore, to be able to see things happening and give reasons about the system, simulation has to take place. SystemC TLM was used to transform a static UML model into an executable model. The executable model providing the opportunity to see the transaction flow within the system objects in an animated manner. In addition, it allowed the simulation of attacks in different parts of the system. The model gives a clear view of the weaknesses in the security requirements, methods, and protocols used in the smart card system.

References

[1] J. Jürjens, "Modelling audit security for smart-card payment schemes with UMLsec," in *Trusted Information: The New Decade Challenge*, M. Dupuy and P. Paradinas, Eds., Paris, 11–13 June 2001, pp. 93–108, proceedings of SEC 2001 – 16th International Conference on Information Security.

[2] S. Schneider, "Security properties and CSP," in *Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on*, 6-8 1996, pp. 174 –187.

[3] J. McDermott, "Visual security protocol modeling," in *NSPW '05: Proceedings of the 2005 workshop on New security paradigms*. New York, NY, USA: ACM, 2005, pp. 97–109.

[4] Object Management Group, "Introduction to OMG's Unified Modeling Language™(UML®)." [Online]. Available: http://www.omg.org/gettingstarted/what_is_uml.htm

[5] J. Jürjens, "UMLsec: Extending UML for secure systems development," in *UML 2002 – The Unified Modeling Language*, pp. 412–425.

[6] ——, "Using UMLsec and Goal-Trees for Secure Systems Development," in *Proceedings of the 2002 ACM symposium on Applied computing*, pp. 1026–1031.

[7] J. Jürjens, J. Schreck, and Y. Yu, "Automated analysis of permission-based security using UMLsec," in *Fundamental Approaches to Software Engineering, 11th International Conference, FASE 2008, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2008, Budapest, Hungary, March 29-April 6, 2008. Proceedings*, 2008, pp. 292–295.

[8] "IEEE Standard System C Language Reference Manual," *IEEE Std 1666-2005*, pp. 0_1 –423, 2006.

[9] K. Rothbart, U. Neffe, C. Steger, R. Weiss, E. Rieger, and A. Muehlberger, "High level fault injection for attack simulation in smart cards," *Asian Test Symposium*, vol. 0, pp. 118–121, 2004.

[10] ——, "Extended abstract: an environment for design verification of smart card systems using attack simulation in SystemC," *Formal Methods and Models for Co-Design, ACM/IEEE International Conference on*, vol. 0, pp. 253–254, 2005.

[11] L. Cai and D. Gajski, "Transaction level modeling: an overview," in *Proceedings of the 1st IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis*, ser. CODES+ISSS '03. New York, NY, USA: ACM, 2003, pp. 19–24.

[12] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. Wiley Publishing, 2008.

[13] W. Rankl, "Overview about attacks on smart cards," *Information Security Technical Report*, vol. 8, no. 1, pp. 67 – 84, 2003.

[14] K. Markantonakis, M. Tunstall, G. Hancke, I. Askoxylakis, and K. Mayes, "Attacking smart card systems: Theory and practice," *Information Security Technical Report*, vol. 14, no. 2, pp. 46 – 56, 2009, smart Card Applications and Security.

[15] K. Baddam and M. Zwolinski, "Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure," in *VLSID '07: Proceedings of the 20th International Conference on VLSI Design held jointly with 6th International Conference*. Washington, DC, USA: IEEE Computer Society, 2007, pp. 854–862.

[16] X. Leng, "Smart card applications and security," *Information Security Technical Report*, vol. 14, no. 2, pp. 36 – 45, 2009, smart Card Applications and Security.

[17] C. Williams, "Configuring enterprise public key infrastructures to permit integrated deployment of signature, encryption and access control systems," in *Military Communications Conference, 2005. MILCOM 2005. IEEE*, 17-20 2005, pp. 2172 – 2175 Vol. 4.