



Ain Shams University
Faculty of Engineering
Computer and Systems Engineering Department

Secure Middleware for ID Smart Cards

Amin Abdel Wahab Amin Sorrour

Master of Science
(Computer and Systems Engineering)
Ain Shams University, 2006

A THESIS
SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE DEGREE OF DOCTOR OF PHILOSOPHY
(Electrical Engineering)
DEPARTMENT OF COMPUTER AND SYSTEMS ENGINEERING

Supervised By
Prof. DR. Mohamed Abdulhamid Sheirah
Prof. Dr. Ayman Mohamed Wahba
Dr. Ayman Mohammad Bahaa-Eldin

Cairo, Egypt
March, 2012



كلية الهندسة

قسم هندسة الحاسبات والنظم

نظام وسيط آمن لبطاقات الهوية الذكية

مقدمة من

أمين عبدالوهاب أمين سرور

ماجستير الهندسة الكهربائية

(هندسة الحاسبات والنظم)

جامعة عين شمس - ٢٠٠٦

رسالة

مقدمة للحصول على درجة دكتوراة الفلسفة في الهندسة الكهربائية

(هندسة الحاسبات والنظم)

تحت إشراف

الأستاذ الدكتور / محمد عبدالحميد شعيرة

الأستاذ الدكتور / أيمن محمد وهبة

الدكتور / أيمن محمد بهاء الدين

القاهرة - مصر

٢٠١٢

بسم الله الرحمن الرحيم

"قالوا سبحانك لا علم لنا إلا ما علمتنا إنك أنت العليم الحكيم"

صدق الله العظيم البقرة ٣٢

بسم الله الرحمن الرحيم

"وقالوا الحمد لله الذي هدانا لهذا وما كنا لنهتدي لولا أن هدانا الله"

صدق الله العظيم الأعراف ٤٣



Faculty of Engineering
Computer and Systems Eng. Dept.

Examiners Committee

Name : Amin Abdel-Wahab Amin Sorrour
Thesis : **Secure Middleware for ID Smart Cards**
Degree : Doctor of Philosophy in Electrical Engineering
(Computer and System Engineering Department)

Name, Title, and Affiliate	Signature
1. Prof. Mohammad Ali Zohdy Electrical and Computer Engineering Dept., Oakland University, USA	
2. Prof. Abdulmoniem A. Wahdan Computer and Systems Engineering Department, Ain Shams University, Egypt	
3. Prof. Ayman M. Wahba Computer and Systems Engineering Department, Ain Shams University, Egypt (Supervisor)	
4. Dr. Ayman M. Bahaa-Eldin Computer and Systems Engineering Department, Ain Shams University, Egypt (Supervisor)	

Date: 2012/05/16

Abstract

Amin Abdel Wahab Amin Sorrour

Secure Middleware for ID Smart Cards

Doctor of Philosophy dissertation

Ain Shams University, 2012

The last surveys indicate that there is an extensive growth in the use of smartcards. A smart card comprises the technology, the platform on which applications are built. An application is a solution to a particular problem. Typically, smart card applications have been being constructed during smart card manufacturing. Nowadays, there is a trend toward building smart card applications after a smart card has been manufactured.

The problem of installing and trusting new applications on smart cards is a critical one, especially for ID smart cards and PKI smart cards, since a new application can be malicious and exposes sensitive information such as private keys and encryption keys from the card.

However, building a trust model for smart cards involve several design issues in both hardware and operating system levels.

In this work, the multi-core processor architecture, typically a dual CPU architecture is utilized as a base for a trusted computing environment. The design is based on dedicating a CPU for secure operations like encryption, decryption, signing and validating of digital signatures. This CPU also is attached to a secure private memory to store critical information such as encryption keys and private certificates. The communication with the other CPU dedicated to run the application is carried out through a 2 port shared memory. A secure loader is built as a part of the smart card OS kernel, where the application is checked for a specific signature before execution.

The trust of an application is guaranteed through requiring any application to be pre-signed with a trusted authority private key. The authority public key is stored in CPU1 private memory.

Based on the model, a trust computing and a new application life cycle are presented. Finally a comparison to the existing state of the art trust models is given.

Keywords:

Secure Computing, Trust Models, Smart Cards, Multi-Core

Preface

With more and more smart card applications being developed, there is a need for the upgrade of current security software on the smartcard. The thesis explores the idea on implementing complex algorithm in the smart card software.

The first chapter explains on the background of smart card technology, smart card standards and the card life cycle.

The second chapter explores on current smart card cryptographic method and the limitation.

The third and fourth chapter elaborates on security technique in the Card Operating System, Access Control systems and authentication techniques. The chapter discusses further on the MTCOS system and how it allows multi application on a single card.

The last two chapters describe the trusted platform for multi-application smart cards and how it is realized using dual processor system with shared memory. The last chapter details the experimental results and conclusion.

Acknowledgements

I would like to express my gratitude to my supervisors, **Prof. DR. Mohamed Abdulhamid Sheirah, Prof. Dr. Ayman Mohammed Wahba and Dr. Ayman Mohammad Bahaa-Eldin** who saved no effort ,time patience, and advice, I recognize that without their motivation and encouragement I would not have finished this research.

I would like to acknowledge and extend my heartfelt to them upon their grateful support, back this success to them.

A very special thanks goes out to **Prof Dr.Abdul Elmoneim Wahdan** for his thoughtful comments and guidance under his focus and vision I developed this thesis.

Finally, I would like to thank **Prof Dr mohammed Ali Zohdy** from the Electrical and Computer Engineering, Oakland University,Rochester, USA for taking time out from his busy schedule to serve as my external reader.

Statement

This dissertation is submitted to Ain Shams University for the degree of Doctor of Philosophy in Electrical Engineering, Computer and Systems

The work included in this thesis was out by the author at Computer and systems Engineering Department, Ain Shams University.

No part of this thesis has been submitted for a degree or qualification at other university or institution.

Date : 16 / /200

Signature :

Name : Amin Abdel Wahab Amin Sorrour

Table of Contents

Abstract	i
Preface	iii
Acknowledgements	iv
Statement	v
List of Tables	ix
List of Figures and Illustrations	x
List of Symbols, Abbreviations and Nomenclature	xii
CHAPTER (1)	xiii
Chapter One:Standards and technologies in Smart Card	1
1.1 Overview	1
1.2 Types of Smart Cards	2
1.2.1 Memory Chip Cards	3
1.2.2 Smart Card Chip	5
1.2.3 Contact-based and Contact-less Smart Cards	8
1.3 Smart Card Operating System	9
1.4 Smart Card Communication	13
1.5 Cryptography and smart card	14
1.6 Standards and Specifications	15
1.7 The smart card life cycle	17
1.8 STRUCTURING DATA	21
Chapter Two:Cryptography & Smart Cards	26
2.1 Smart card limitations.....	26
2.2 Cryptographic Primitives.....	28
2.2.1 Symmetric Ciphers	29
2.2.2 Hash & MAC functions.....	32
2.2.3 Asymmetric Ciphers	33
2.2.4 System components:	35
2.2.5 System components description:	36
2.2.6 Applications.....	39
Chapter Three:Security techniques in COSs.	43
3.1 Internal Authentication	43
3.2 External Authentication.....	44
3.3 PIN Verification	45
3.4 Operational Support/Technical Considerations.....	46
3.4.1 Personalization Process	46
3.5 Application Loading	47
3.6 Technical implementation	47
3.7 Securing multi-applications and protection.....	48

3.7.1	Securing Multi-application.....	49
3.8	Multi Application Card Operating Systems (MACOS)	49
3.9	Privacy Protection	51
3.10	Basic issues of Secure and Identification Applications.....	52
3.10.1	National IDs.....	52
3.10.2	E-voting	53
3.10.3	E-Passport.....	54
3.10.4	Identity fraud	58
3.10.5	Securing your information.....	58
3.11	Access Control (BAC).....	60
3.12	Extended Access Control (EAC).....	61
3.12.1	Passive Authentication (PA).....	63
3.13	Active Authentication(AA)	64
3.14	Chip Threat Analysis	68
3.14.1	Lost and Stolen Chips.....	68
3.14.2	Lost and Stolen Passport Bodies (pre-chip)	68
3.14.3	Lost and Stolen Completed Passport Bodies	69
3.14.4	Lost and Stolen – Issued Passports.....	69
3.14.5	Modification of Data on the Chip.....	69
Chapter Four:	Smart Card Operating System & MTCOS	72
4.1	What is the COS?	72
4.2	Smart Card Operating System Design.....	73
4.2.1	Smart Card Command Processing.....	74
4.2.2	Commercial Smart Card Operating Systems.....	76
4.2.3	Java Card Platform	76
4.2.4	MULTOS OS Platform.....	79
4.3	MTCOS Overview.....	81
4.3.1	Files	82
4.3.2	4.2.1 File Type.....	83
4.3.3	File Structure	84
4.3.4	Access Conditions	85
4.3.5	Life Cycle	86
4.4	Communication & APDU issues.....	87
4.5	Memory	92
4.6	Applications.....	96
4.7	IBM High Assurance Smart- Card OS	100
4.8	Persistent Storage Manager - PSM.....	109
4.9	Implementing Application Download	113
4.10	Cryptographic Challenges	115
4.11	Chip Initialization.....	117
Chapter Five:	Trusted Platform for Multi-Application Smart Cards	121

5.1	Introduction	121
5.2	Trust Platform.....	122
5.2.1	Dual CPU Hardware System	125
5.2.2	Crypto Engine and PKI	134
5.2.3	Trusted Application Model.....	136
5.3	Comparison with the state of the art.....	139
Chapter Six:Experimental Results		143
6.1	Hardware Realization	143
6.1.1	RTL (register transfer level) view	143
6.1.2	Low level system view (system interconnection).....	145
6.1.3	Flow summary report	146
6.1.4	Hand shaking diagram	146
6.2	Performance Evaluation	147
Chapter Seven:Conclusion and Future work		149
7.1	Conclusion	149
7.2	Future work	149
References		151

List of Tables

Table 1-1 Summary of the individual life-cycle phases according to the ISO 10202-1 standard.....	18
Table 5-1 modular reduction algorithm.....	128
Table 5-2 Sign possibilities	131
Table 5-3 Worst case sign	132
Table 5-4 Modular Reduction Algorithm.....	133
Table 5-5 Implementation results	134
Table6.1 Flow summary report	146

List of Figures and Illustrations

Figure 1.1 : Smart Card Types	3
Figure 1.2: Architecture of a Smart Card chip	6
Figure 1.3: Purpose of Smart Card Contacts	9
Figure 1.4 Generic Multi-Application Operating System Architecture ...	11
Figure 1.5 : ISO 7816 Parts 1-8.....	17
A simple example of data type definition using ASN. 1	22
Figure : 1.6 TLV encoding of the name "Amin"	23
Figure 1.7 Basic scheme for forming constructed TLV-coded data structures from several primitive TLV-coded data objects. The indices ‘C’ and ‘P’ stand for ‘constructed’ and ‘primitive’	24
Figure 2.1: Challenge-Response Model	30
Figure 3.1 Internal Authentication	44
Figure 3.2 External Authentication	45
Figure 3.3: Basic Access Control	60
Figure 3.4: Extended Access Control.....	61
Figure 3.5: Passive Authentication.....	63
Figure 3.6: Active Authentication	64
Figure 4.2: Java Card Organization.....	77
Figure 4.3: CardLet Development and Installation	78
Figure 4.4: MULTOS OS Platform	80
Figure 4.5 Overview MTCOS	82
Figure 4.8: Data Memory Space Architecture.....	93
Figure 4.9: Directory Structure Implementation.....	102
Figure 4.10: PCM Memory Objects For Files.....	103
Figure 4.11: PSM Use of Persistent Storage.....	110
Figure 5.1 Trust Platform System	124
Figure 5.2 Dual CPU Hardware System.....	125
Figure 5.3 Sign Detection.....	129
Figure 5.4 Trusted Loader	138
Figure 6.1 RTL view	144

Figure 6.2 Low level system view	145
Figure 6.3 Hand shaking diagram	146