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 الكهربية
(هندسة الحاسبات والنظم)
جامعة عين شمس – ٢٠٠٦

رسالة
مقدمة للحصول على درجة دكتوراة الفلسفة في الهندسة الكهربية
(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

List of Tables

List of Figures and Illustrations