Design and Implementation of Public Key Infrastructure on Smart Card Operating System

by

Aditi Gupta

Department of Computer Science and Engineering
Indian Institute of Technology
Kanpur – 208 016

MAY 2008

Design and Implementation of Public Key Infrastructure on Smart Card Operating System

A Thesis
Submitted in partial fulfilment of the
requirements for the Degree of
Master of Technology

by

Aditi Gupta

to the
Department of Computer Science and Engineering
Indian Institute of Technology
Kanpur – 208 016

MAY 2008

Certificate

It is certified that the work contained in the thesis entitled "Design and implementation of public key infrastructure on smart card operating system", by "Aditi Gupta", has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

Dr. Rajat Moona,
Department of Computer Science and Engineering,
Indian Institute of Technology, Kanpur.

May, 2008

Abstract

Smart cards are an ideal medium for use in secure applications. Such applications require mechanisms for cryptographic authentication, password based authentication, confidential data exchange, detection of data tampering and verification of origin integrity. Cryptographic techniques based on symmetric key algorithms and/or public key cryptography can be used to address these issues. In this thesis, we focus on development of public key infrastructure on smart cards. Public key cryptography provides easier key management since keys are assigned on per user basis as opposed to per communication pair basis as in the case of symmetric key cryptography. Further, the public key cryptography can be used to perform key exchange for symmetric key and then the symmetric key cryptography can be used to perform further cryptographic operations. Smart cards are secure devices since the keys are kept in it securely and only the operations using such keys are permitted to be performed.

We propose a comprehensive design for development of public key infrastructure on smart cards. This design is compliant to ISO/IEC-7816 international standards for smart cards [2–9] and the SCOSTA-CL specification [1]. We have implemented features like encryption/decryption schemes, storage and retrieval of cryptographic information etc. on the smart card operating system as per our design specifications.

Acknowledgements

I would like to express my gratitude towards my thesis supervisor, Dr. Rajat Moona, for his invaluable guidance and support in completing this thesis work. His enthusiasm, innovative suggestions and deep insight into technical matter were instrumental in the conceptualization of this work. Working under his supervision was a great learning experience. I would also like to thank him for initiating my interest in the areas of operating system and system security.

I would like to thank all the people who have been a part of SCOSTA lab for their assistance during various phases of the project. I would like to thank my friends Srishti and Pragya for their patience in reviewing my report and providing valuable feedback. I truly enjoyed working with them.

I would like to thank all my friends for always being by my side and making my stay here truly enjoyable and memorable. I'll always cherish the moments I spent with them. I would also like to thank my institute and my department for providing me with the best facilities and a wonderful work environment. I would like to thank all my professors for their words of wisdom and guidance throughout my stay here.

Finally, I would like to express my gratitude towards my parents and my brother for their love, support and encouragement in all my endeavours.

Contents

List of Figures

List of Tables

Abbreviations

AID	**A**pplication **I**dentifier
AM	**A**ccess **M**ode
APDU	**A**pplication **P**rotocol **D**ata **U**nit
ASN.1	**A**bstract **S**yntax **N**otation **O**ne
AT	**A**uthentication **T**emplate
ATQA	**A**nswer **T**o Re**q**uest Type-**A**
ATR	**A**nswer **T**o **R**eset
ATS	**A**nswer **T**o **S**elect
BER	**B**asic **E**ncoding **R**ules
CA	**C**ertifying **A**uthority
CBC	**C**ipher **B**lock **C**haining
CCA	**C**entral **C**ertifying **A**uthority (Root-CA)
CCT	**C**ryptographic **C**hecksum **T**emplate
CDE	**C**ryptographic **D**ata **E**lement
CIA	**C**ryptographic **I**nformation **A**pplication
CIO	**C**ryptographic **I**nformation **O**bject
CRT	**C**ontrol **R**eference **T**emplate
CT	**C**onfidentiality **T**emplate
DDO	**D**iscretionary **D**ata **O**bject
DER	**D**istinguished **E**ncoding **R**ules
DES	**D**ata **E**ncryption **S**tandard
DF	**D**edicated **F**ile
DF.CIA	**D**edicated **F**ile containing **CIA**
DH	**D**iffie-**H**ellman key exchange protocol
DO	**D**ata **O**bject
DSA	**D**igital **S**ignature **A**lgorithm
DST	**D**igital **S**ignature **T**emplate
EF	**E**lementary **F**ile

EF.AOD	**A**uthentication **O**bject **D**irectory
EF.PrKD	**P**rivate **K**ey **D**irectory
EF.PuKD	**P**ublic **K**ey **D**irectory
EF.SKD	**S**ecret **K**ey **D**irectory
EF1	Represents internal record **EF** with SFID = **1**
EF2	Represents internal record **EF** with SFID = **2**
FCP	**F**ile **C**ontrol **P**arameters
HT	**H**ash **T**emplate
ICC	**I**ntegrated **C**ircuit **C**ard
IFD	**I**nterface **D**evice
KAT	**K**ey **A**greement **T**emplate
Lc	**L**ength of **c**ommand data in a command APDU
Le	Maximum **l**ength of data **e**xpected in APDU from the ICC as a response to command APDU
MAC	**M**essage **A**uthentication **C**ode
MF	**M**aster **F**ile
OD	**O**bject **D**irectory
OS	**O**perating **S**ystem
P1	First parameter byte for the APDU
P2	Second parameter byte for the APDU
PCD	**P**roximity **C**oupling **D**evice
PICC	**P**roximity **I**ntegrated **C**ircuit **C**ard
PKC	**P**ublic **K**ey **C**ryptography
PKCS	**P**ublic **K**ey **C**ryptography **S**tandard
PKI	**P**ublic **K**ey **I**nfrastructure
PPS	**P**rotocol and **P**arameters **S**election
PSO	**P**erform **S**ecurity **O**peration
RATS	**R**equest for **A**nswer **T**o **S**elect
REQA	**Req**uest Type-**A**
RSA	**R**ivest-**S**hamir-**A**dleman algorithms for Public-Key Cryptography
SAK	**S**elect **A**c**k**nowledge
SC	**S**ecurity **C**ondition
SE	**S**ecurity **E**nvironment
SHA1	**S**ecure **H**ash **A**lgorithm variant **1** (Message Digest Algorithm)

SW1	First byte of the **s**tatus **w**ord in the response APDU
SW2	Second byte of the **s**tatus **w**ord in the response APDU
TLV	**T**ag **L**ength **V**alue
UID	**U**nique **I**dentifier
WUPA	**W**ake **Up** Type-**A**

Chapter 1

Introduction

Integrated circuit cards (ICC) or smart cards are credit-card sized plastic cards [15] embedded with a memory chip for data storage and optionally a microprocessor to provide processing capabilities. Smart cards which provide only data storage capabilities are known as memory based smart cards; while smart cards which also have processing capabilities are known as microprocessor based smart cards. A microprocessor based smart card executes a software component such as an operating system and hence complex logic and algorithms can be built into it. In this document, the term "smart card" shall be used to refer implicitly to a microprocessor based smart card. The interaction with a smart card is carried out using a specialized hardware called an interface device (IFD) or a smart card reader as a more commonly used name. A smart card does not have its own power supply and needs an external power source to power it up. This external power is supplied by the smart card reader. The communication between a smart card and a reader can occur either in contact-mode or in contact-less mode. In contact-mode, the contact card is inserted into the reader with a mating contact and the electric circuit completed due to this physical contact is used to power up the card. In contact-less mode, the contact-less card is placed in the RFID-field of the reader which is then used to power up the card. Smart cards are small and easy to handle devices which make them very usable in everyday applications.

Security is a major concern in many everyday applications like e-Commerce [15, 31, 32] etc. Most of these applications require secure and confidential data exchange [15, 21, 30], mechanisms to detect tampering/modification of data [15, 21, 28, 30], verification of origin integrity [15, 21, 25, 30] etc. Various cryptographic

mechanisms are required to establish a secure trusted environment or to operate securely in a non-trusted medium. These requirements can be addressed by use of either symmetric-key based or asymmetric-key based cryptographic techniques. A public key infrastructure (PKI) is a framework which uses the capabilities of performing asymmetric key cryptography, also known as public key cryptography (PKC). PKC involves a pair of cryptographic keys called private and public keys. A private key is known only to the owner of the key while the public key can be distributed freely. Decryption and signature computation are two operations that are performed by an entity using its private key while encryption and digital signature verification operations are carried out using the corresponding public key. PKI builds over the PKC to support functionality such as digital signatures, origin integrity, certificates for the genuineness of the public key etc.

Smart cards are an ideal medium for use with PKI applications. Smart cards provide secure storage of confidential data and are capable of executing complex cryptographic algorithms. They provide secure storage for private keys and are resistant to tampering. Some smart cards have dedicated co-processors (crypto-processors) for executing cryptographic algorithms which make cryptographic computations much faster and efficient. Smart cards can be used as authorization media and encryption modules. They offer high degree of reliability and safeguard against unauthorized modification of protected data like private keys.

1.1 Motivation

A smart card may operate in either contact-mode or in contactless-mode. Security concerns increase when the card is operating in contactless-mode because attacks like eavesdropping [21, 29, 30] and man-in-the-middle [21, 29, 30] become feasible. The situation is analogous to enhanced security issues in wireless networks compared to wired networks. Eavesdropping and man-in-the-middle attacks are also possible in contact-mode of communication by modifying interface between the smart card and the reader. In man-in-the-middle attack, the attacker sits between two communicating parties and modifies the message being exchanged without the sender or receiver of the message knowing about it. Eavesdropping is an attack in which the attacker reads the ongoing communication between two parties. In our scenarios, the two parties are the smart card and the reader.

Tampering of data can be prevented only by physically securing the medium of communication which is not possible when the card is operating in contactless-mode. However, it is possible to detect the modification of data by incorporating either cryptographic checksum [21, 28] or digital signature [24, 25]. The computation and verification of digital signature [24, 25] involves the use of private-public key pair.

Eavesdropping can be prevented by encrypting the data that is to be transmitted using either session keys or derived keys. However, derived keys are not very secure because if the data to derive the key is exchanged in plain text, there is a possibility that the attacker intercepts this data and establishes separate session keys with both communicating parties. In that case, all conversation is routed through this attacker and the encryption becomes useless. Certain well known mechanisms of key exchange such as Diffie Hellman key exchange [21] protocol suffer from this weakness. The session key establishment using PKI requires performing encryption and decryption of key-material using public and private keys respectively. Exchanging this key material in encrypted form makes it resistant to man-in-the-middle attack.

Since public keys are publicly available, they can be easily modified or replaced with some other entity's public key. We need a mechanism to verify the genuineness of a public key, i.e. to check if the public key actually belongs to a particular user or not. A public key can be associated with a user by embedding the public key in a certificate [12] which is then digitally signed by a higher authority known as the certification authority (CA). A certificate includes the digitally signed information such as the name of the owner, duration of certificate validity, public key etc. The public key required for encryption or signature verification can be extracted from its corresponding certificate after performing certificate verification with the CA's trusted public key. The certificate processing is a part of the PKI. Hence, the development of a public key infrastructure on smart cards is needed. This enhances the security of critical information.

Nowadays, smart cards are being extensively used in a wide variety of applications ranging from simple identification cards to secure electronic passports. They are being deployed in applications involving financial transactions like bank cards, electronic purses and credit cards. Smart cards are also being used as secure data storage medium and also as access control systems for restricted areas and computers. Some countries use smart cards as rechargeable electronic tickets for

transport applications. In India, smart cards are being used as driving license in certain states [1, 33]. Smart cards are also being deployed in electronic passports [1, 34] in various countries including India. Critical applications like e-Passports, credit cards etc. require a very robust and sophisticated security infrastructure to safeguard them from malicious attacks. A public key infrastructure can go a long way in addressing these security issues and make secure applications robust against various attacks like eavesdropping or man-in-the-middle attack.

1.2 Related Work

The ISO/IEC-7816 standards [2–9] are international standards related to smart cards. These standards cover almost every aspect of smart card operation. However, due to their extensive nature, they are not specific enough in certain areas and can be interpreted in more than one way. SCOSTA-CL specifications [1] which were developed jointly by IIT Kanpur and National Informatics Center, India, further refine the ISO specifications to remove ambiguous behavior and provide for inter-operability of smart cards when implemented by any smart card OS developer. A smart card operating system compliant to SCOSTA specifications was developed at IIT Kanpur in 2001 [17] and was initially intended for transport applications for identity and security. This OS has been extended over the years and more functionality has been added to it. The current OS implementation is compliant to the SCOSTA-CL specifications and ISO/IEC-7816 standards. SCOSTA OS has a well designed file structure and security architecture in place. It supports both contact and contact-less communication protocols. It also has support for symmetric key cryptography, secure messaging, various authentication mechanisms and session key establishment protocols based on symmetric key operations.

None of the above mentioned developments, however, incorporate public key cryptography. An attempt to design and implement PKI on SCOSTA OS was made by Venkat Rao Pedapati and Sri Simil Dutta in 2007 [16]. However their design addressed only a small part of PKI and was not compatible with ISO/IEC-standards. Their major contribution to SCOSTA-OS was developing modular exponentiation using crypto-processor in hardware which is the most time consuming and crucial part of public key cryptography. Several researchers have worked on PKI using smart cards. Markantonakis and Mayes [19] in 2005 proposed a secure channel

protocol for multi-application smart cards which is based on public key cryptography. Fuchsberger et. al. [20] surveyed the mathematical techniques behind development of public key cryptography in smart cards, compared digital signature schemes and discussed security management issues of smart card production. Jean Francois Dhem [18] designed an efficient public key cryptography library in 1998 for use in RISC-based smart cards.

1.3 Thesis Objective

As part of this thesis, we developed and defined a comprehensive Public Key Infrastructure (PKI) on smart cards. The specifications proposed by us for incorporating public key cryptography support in smart cards are referred to as SCOSTA-PKI. The SCOSTA-PKI specifications are compatible with the ISO/IEC 7816 standards and are built over the SCOSTA-CL standard [1]. The design of SCOSTA-PKI clearly outlines the various operations required in PKI like encryption, decryption and digital signature computation and also specifies the basic data structure to store and retrieve cryptographic information from the cards. It describes protocols for authentication and mechanisms to establish session keys. It also specifies the cryptographic algorithms that an OS must support but does not limit an OS to just those algorithms. The SCOSTA-PKI design is a generic and implementable design which can be used by any developer as a reference while developing PKI functionality on their OS. It explains the design of PKI on smart cards in its entirety while at the same time giving opportunity to extend and incorporate newer algorithms.

We have also extended the existing OS implementation to support the PKI mechanisms as outlined in SCOSTA-PKI. We implemented the basic data structures to store and retrieve keys and passwords from the card over the existing security architecture. The cryptographic information is stored in a different manner in SCOSTA-PKI when compared to the SCOSTA-CL. Maintaining the backward compatibility with SCOSTA-CL operating system was very crucial while incorporating newer functionality in it. Various commands and algorithms for encryption, decryption and signature computation were also implemented.

1.4 Thesis Organization

The rest of this thesis is organized as follows. We discuss the relevant background in chapter 2 where we describe the public key cryptography and explain the basic features of the SCOSTA operating system. In chapter 3, we discuss the design of PKI as developed and formulated by us in SCOSTA-PKI specifications and discuss basic data structures, operations like encryption, decryption, signature computation, certificate verification and various protocols for authentication and session key establishment. The implementation details are outlined in chapter 4. We discuss the test methods used to test the SCOSTA-PKI operating system in chapter 5. We then conclude this work in chapter 6.

Bibliography

[1] IIT Kanpur and NIC India, *SCOSTA-CL Specifications v1.2: Specifications for the Smart-Card Operating System with Contact-less Interface*,Version 1.2, available online at http://www.scosta.gov.in, India, July 2007

[2] ISO/IEC 7816-3:1997, *Identification cards – Integrated circuit cards – Part 3: Electronic signals and transmission protocols*, 2nd Edition, Geneva, Switzerland, 1997.

[3] ISO/IEC 7816-4:1995, *Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange*, 1st Edition, Geneva, Switzerland, 1995.

[4] ISO/IEC 7816-4:2005, *Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange*, 2nd Edition, Geneva, Switzerland, 2005.

[5] ISO/IEC 7816-5:2003, *Identification cards – Integrated circuit cards – Part 5: Registration of application identifiers*, 2nd Edition, Geneva, Switzerland, 2003.

[6] ISO/IEC 7816-6: 1996, *Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange*, 1st Edition, Geneve, Switzerland, 1996.

[7] ISO/IEC 7816-8: 1999, *Identification cards – Integrated circuit cards – Part 8: Commands for security operations*, 1st Edition, Geneva, Switzerland, 1999.

[8] ISO/IEC 7816-9: 2000, *Identification cards – Integrated circuit cards – Part 9: Commands for card management*, 1st Edition, Geneva, Switzerland, 2000.

[9] ISO/IEC 7816-15: 2004, *Identification cards – Integrated circuit cards – Part 15: Cryptographic Information Application*, 1st Edition, Geneva, Switzerland, 2003.

[10] PKCS #1 v2.1:2002 *RSA Cryptography Standard*, RSA Laboratories, Version 2.1, available online at ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf, Bedford, USA, June 2002.

[11] PKCS #3: 1993 *Diffie-Hellman Key-Agreement Standard*, RSA Laboratories, Version 1.4, available online at ftp://ftp.rsasecurity.com/pub/pkcs/ps/pkcs-3.ps, Redwood City, USA, November 1993.

[12] PKCS #6: 1993 *Extended-Certificate Syntax Standard*, RSA Laboratories, Version 1.5, available online at ftp://ftp.rsasecurity.com/pub/pkcs/ps/pkcs-6.ps, Redwood City, USA, November 1993.

[13] PKCS #15 v1.1:2000 *Cryptographic Token Information Syntax Standard*, RSA Laboratories, Version 1.1, available online at ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-15/pkcs-15v1_1.pdf, Bedford, USA, June 2000.

[14] RFC 3280:2002 *Internet X.509 Public Key Infrastructure: Certificate and CRL Profile*, available online at http://www.ietf.org/rfc/rfc3280.txt, The Internet Society, April 2002.

[15] W. Rankl and W. Effing, *Smart Card Handbook*, 3rd Edition, John Wiley & Sons Ltd, West Sussex, England, January 2004.

[16] V. Pedapati and S. Dutta, "Design and Implementation of Public Key Infrastructure in SCOSTA," B.Tech. Project Report, Indian Institute of Technology, Department of Computer Science, Kanpur, India, April 2007

[17] R. Shankesi, "Development of an operating system for smart cards," M.Tech. Dissertation, Indian Institute of Technology, Department of Computer Science, Kanpur, India, May 2002.

[18] J. F. Dhem, "Design of an efficient Public-Key Cryptographic Library for RISC based Smart Cards," Ph.D. Dissertation, University Catholique de Louvaln, Belgium, May 1998.

[19] K. Markantonakis and K. Mayes, "A Secure Channel Protocol for Multi-Application Smart Cards Based on Public Key Cryptography," *IFIP International Federation for Information Processing*, vol. 175, pp. 79-95, Springer Boston, Oct. 2005.

[20] A. Fuchsberger, D. Gollmann, P. Lothian, K. G. Paterson and A. Sidiropoulos, "Public-key cryptography on smart cards," *Proceedings of the International Conference on Cryptography: Policy and Algorithms*, vol. 1029, pp. 250-269, 1995.

[21] W. Stallings, *Cryptography and Network Security*, 4th Edition, Pearson Prentice Hall, Upper Saddle River, NJ, USA, 2006.

[22] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, pp. 644-654, November 1976.

[23] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete algorithms," *IEEE Transactions on Information Theory*, vol. 31, pp. 469-472, July 1985.

[24] US Department of Commerce - National Institute of Standards and Technology, *FIPS PUB 186: Digital Signature Standard (DSS)*, May 1994.

[25] 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, February 1978.

[26] N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, vol. 48, No. 177, pp. 203-209, January 1987.

[27] V. Miller, "Use of elliptic curves in cryptography," *Lecture notes in computer sciences; 218 on Advances in cryptology - CRYPTO 85*, pp. 417 - 426, June 1986.

[28] F. Cohen, "A Cryptographic Checksum for Integrity Protection," *Computers and Security*, vol. 6, Issue 6, pp. 505-510, December 1987.

[29] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*, 2nd Edition, John Wiley & Sons Inc., New York, USA, 1995.

[30] C. Kaufman and R. Perlman and M. Speciner, *Network security: private communication in a public world*, Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1995.

[31] A.K. Ghosh, *E-Commerce Security: Weak Links, Best Defenses*, John Wiley & Sons, January 1998.

[32] A.K. Ghosh and T.M. Swaminatha, "Software security and privacy risks in mobile e-commerce," *Communications of the ACM*, vol. 44, No. 2, pp. 51-57, New York, USA, February 2001.

[33] Parivahan — National Transport Informatics Division, *http://www.parivahan.nic.in*

[34] A. Juels and D. Molnar and D. Wagner, "Security and Privacy Issues in E-passports," *SECURECOMM'05*, pp. 74-88, IEEE Computer Society , 2005.

[35] ISO/IEC 9797-1:1999, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*, 1st Edition, Geneva, Switzerland, 1999.

[36] ISO/IEC 14443-3:2001, *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision*, 1st Edition, Geneva, Switzerland, 2001.

[37] ISO/IEC 14443-4:2001, *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol*, 1st Edition, Geneva, Switzerland, 2001.

[38] US Department OF Commerce - National Institute of Sandards and Technology, *FIPS PUB 46-3: Data Encryption Standard (DES)*, October 1999.

[39] ISO/IEC 11770-2:1996, *Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques*, 1st Edition, Geneva, Switzerland, 1996.

[40] US Department OF Commerce - National Institute of Sandards and Technology, *FIPS PUB 140-2: Security requirements for cryptographic modules*, May 2001.

[41] O. Dubuisson, *ASN.1 - Communication Between Heterogeneous Systems*, 1st Edition, Morgan Kaufmann Publishers, September 2000.

[42] NXP Semiconductors, *P5CD036 Secure Dual Interface PKI smart card controller - Product Datasheet*, Rev. 3.0, March 2006.

[43] NXP Semiconductors, *P5CD072 Secure Dual Interface PKI smart card controller - Product Datasheet*, Rev. 3.0, March 2006.

[44] NXP Semiconductors, *P5CD036 Secure Dual Interface and contact PKI smart card controller - Product Datasheet*, Rev. 3.3, August 2007.