SMART CARD TECHNOLOGY

WONG KIUNG CHUNG

Universiti Malaysia Sarawak
1998

Borang Penyerahan Tesis
Universiti Malaysia Sarawak

R13a

BORANG PENYERAHAN TESIS

Judul: SMART CARD TECHNOLOGY

SESI PENGAJIAN: 1998/1999

Saya WONG KIUNG CHUNG
(HURUF BESAR)

mengaku membenarkan tesis ini disimpan di Pusat Khidmat Maklumat Akademik, Universiti Malaysia Sarawak dengan syarat-syarat kegunaan seperti berikut:

1. Hakmilik kertas projek adalah di bawah nama penulis melainkan penulisan sebagai projek bersama dan dibiayai oleh UNIMAS, hakmiliknya adalah kepunyaan UNIMAS.
2. Naskhah salinan di dalam bentuk kertas atau mikro hanya boleh dibuat dengan kebenaran bertulis daripada penulis.
3. Pusat Khidmat Maklumat Akademik, UNIMAS dibenarkan membuat salinan untuk pengajian mereka.
4. Kertas projek hanya boleh diterbitkan dengan kebenaran penulis. Bayaran royalti adalah mengikut kadar yang dipersetujui kelak.
5. * Saya ~~membenarkan~~/tidak membenarkan Perpustakaan membuat salinan kertas projek ini sebagai bahan pertukaran di antara institusi pengajian tinggi.
6. ** Sila tandakan (✓)

☐	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972).
☐	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/ Badan di mana penyelidikan dijalankan).
☑	TIDAK TERHAD	

(TANDATANGAN PENULIS)

Alamat tetap: 9C 1ST FLOOR
EMPLAM LANE 96000
SIBU SARAWAK

Tarikh: 20 HB. SEPTEMBER, 1998

Disahkan oleh

(TANDATANGAN PENYELIA)

MR. NG LIANG YEW
Nama Penyelia

Tarikh: 20 HB. SEPTEMBER, 1998

CATATAN * **Potong yang tidak berkenaan.**
** **Jika Kertas Projek ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa/ organisasi berkenaan dengan menyertakan sekali tempoh kertas projek. Ini perlu dikelaskan sebagai SULIT atau TERHAD.**

Tesis ini telah dibaca dan disahkan oleh:

Mr. Ng Liang Yew

20/9/98

Tarikh

Penyelia

SMART CARD TECHNOLOGY

WONG KIUNG CHUNG

Tesis Dikemukan Kepada
Fakulti Kejuruteraan, Universiti Malaysia Sarawak
Sebagai Memenuhi Sebahagian daripada Syarat
Penganugerahan Sarjana Muda Kejuruteraan
Dengan Kepujian (Kejuruteraan Elektronik dan Telekomunikasi)
September 1998

Dedicated to my beloved family and friends.

ACKNOWLEDGEMENT

First of all, I would like to express my high gratitude to Mr. Ng Liang Yew, supervisor of my thesis, who has given me a lot of guidance and encouragement.

Also, special thanks are directed to my friends, who have given me a lot of support during the completion of this dissertation. Special thanks to Alexander Siew, Chowei, H. S. Goh, P. H. Teoh who have been supportive friends and gone through this hard time together with me.

To my beloved family, I am grateful for their support and guidance throughout these years. Without them, I will never be here in UNIMAS.

Finally, thank to the God Almighty for He has provided me with strength and intelligence to go through all these difficulties.

ABSTRACT

Smart Card technology is a new technology. It has been first developed to solve the problem of fake credit cards. This paper gives an overview on smart card technology. At first, this paper gives the history of smart card technology development. Then, the standard related to this technology is introduced. There are three layers for the data transmission between the smart card and the terminal. But, only the layer two and layer three are emphasized in this paper. Different technologies are used to enhance the security feature of smart card. Some of them are introduced in this paper in brief. Manufacturing process of smart card gives a reader an idea how a smart card is made with all the processes involved. A few examples of smart card application are given. Finally, 8051 microcontroller, the core of the smart card is discussed.

ABSTRAK

Teknologi Kad Pintar ialah teknologi baru. Ia telah dicipta untuk menyelesaikan masalah kad kredit palsu. Kertas ini akan memberi gambaran secara keseluruhan kepada teknologi ini. Pada mulanya, kertas ini akan menceritakan sejarah bagi pembangunan teknologi kad pintar. Selepas ini, piawaian bagi teknologi ini akan diperkenalkan. Terdapat tiga lapisan untuk penghantaran data di antara kad pintar dan pangkalannya. Tetapi, hanya lapisan dua dan lapisan tiga dipentingkan dalam kertas ini. Pelbagai teknologi telah digunakan untuk mengukuhkan lagi ciri-ciri keselamatan kad pintar. Sebahagian sahaja yang diperkenalkan dalam kertas ini secara ringkas. Proses pembuatan kad pintar memberi pembaca satu idea bagaimana satu kad pintar dibuat dengan semua proses yang terlibat. Beberapa contoh kegunaan kad pintar telah diberikan. Akhirnya, *8051 microcontroller*, bahagian yang terpenting dalam kad pintar dibincangkan.

TABLE OF CONTENTS

		Page
APPROVAL LETTER		
APPROVAL SHEET		
PROJECT TITLE		
DEDICATION		ii
ACKNOWLEDGEMENT		iii
ABSTRACT		iv
ABSTRAK		v
TABLE OF CONTENTS		vi
LIST OF TABLES		xi
LIST OF FIGURES		xii
Chapter		
1	INTRODUCTION	1
	1.1 History	1
	1.2 Smart Card	3
2	STANDARDS FOR SMART CARDS	7
	2.1 ISO 7810 Identification Cards – Physical Characteristics	8
	2.2 ISO 7811 Identification Cards – Recording	

Techniques 10

2.3 ISO 7812-1 Identification Cards – Identification of Issuers – Part 1: Numbering System 11

2.4 ISO 7816 Identification Cards – Integrated Circuit(s) Cards with Contacts 12

2.4.1 Part 1: Physical Characteristics 12

2.4.2 Part 2: Dimensions and Location of the Contacts 15

2.4.3 Part 3: Electronic Signals and Transmission Protocols 17

3 DATA TRANSMISSION TO THE SMART CARD 22

3.1 Physical Transmission Layer 24

3.2 Transmission Protocols 25

3.2.1 Transmission Protocol T=0 26

3.2.2 Transmission Protocol T=1 31

3.2.2.1 Block Structure 32

3.2.2.2 Waiting Times 35

3.2.2.3 Protocol Control Byte 38

3.2.3 Comparison of Asynchronous Transmission Protocols 42

3.2.4 Answer To Reset (ATR) 43

3.2.5 Protocol Type Selection (PTS) 54

3.3 Application-Layer Protocols 56

3.3.1 Instruction APDU Structure 57

3.3.2 Response APDU Structure 59

4 SECURITY

4.1 Hardware Enhancement 60

4.2 Personal Identification Number (PIN) 61

4.3 Advanced Cryptography Algorithms 61

4.3.1 Symmetric Authentication 62

4.3.2 Asymmetric Authentication 63

4.3.3 Digital Signature 64

4.4 Biometrics 65

4.4.1 Physiological Features 65

4.4.2 Behavioural Features 67

5 MANUFACTURING OF SMART CARD 69

5.1 Chip and Module 69

5.1.1 Software Engineering 70

5.1.2 Wafer Manufacturing 72

5.1.3 Microprocessor Testing 73

5.1.4 Wafer Cutting 73

5.1.5 Die Incorporation in Modules 73

5.1.6 Bonding 74

5.1.7 Protective Coat 75

5.1.8 Module Testing 75

5.2 Card Body 76

5.2.1 Foil Printing 76

5.2.2 Card Body Manufacturing 77

5.2.3 Milling of Module Cavity 77

5.2.4 Module Incorporation 78
5.3 Smart Card 78
5.3.1 Electrical Test 78
5.3.2 Completion 79
5.3.3 Initialization 79
5.3.4 Personalization 79

6 APPLICATIONS OF SMART CARD 81
6.1 Electronic Purse 81
6.2 Telecommunications 82
6.3 Mobile Communications 82
6.4 Public Transportation 83
6.5 Smart Card in Airline Industry 83
6.6 Medical/Health Services 84
6.7 College Campuses 84

7 THE 8051 MICROCONTROLLER 86
7.1 The 8051 Microcontroller Family Architecture 87
7.2 On-chip Memory 93
7.2.1 Random Access Memory (RAM) 93
7.2.2 Read Only Memory (ROM) 94
7.2.3 External Memory 95
7.3 Development of A Microncontroller-Based System 95
7.3.1 Software Development 96
7.3.2 Hardware Development 97
7.3.3 Integration and Verification 99

7.4 Building an 8051-Based Microcontroller System 100

7.4.1 The CPU Subsystem 101

7.4.2 The Memory Block 103

7.4.3 The Input/Output Block 103

8 FUTURE DEVELOPMENT 106

9 CONCLUSION 109

APPENDIX 111

REFERENCES 115

LIST OF TABLES

Table		Page
2.1	ISO standards pertaining to Smart Cards	9
2.2	Exposure limits for physical phenomena	13
2.3	Contact definitions for Smart Cards	17
2.4	Contact states prior to card reset	19
3.1	Overview of transmission protocols covered by ISO/IEC 7816-3	26
3.2	CLA instruction set definitions	29
3.3	ISO/IEC 7816-4 INS codes	30
3.4	SW1 various error conditions	31
3.5	T=1 transmission block structure	32
3.6	Steps in T=1 error detection and processing	42
3.7	Comparison of asynchronous transmission protocols, conforming to international standards	42
7.1	Comparison of MCS-51™ ICs	87
7.2	Alternate pin functions for port pins	90
7.3	Register values after system reset	92
7.4	List of the 8051 SFRs	94

LIST OF FIGURES

Figure		Page
1.1	Typical architecture of a memory card with security logic	4
1.2	Typical architecture of microprocessor cards	5
2.1	Relationship between the different card formats ID-1, ID-00 and ID-000	8
2.2	The ID-1 format	10
2.3	Embossing and magnetic stripe locations	11
2.4	Static electricity test	13
2.5	Bending properties test	14
2.6	Torsion testing of a Smart Card	15
2.7	Minimum size of contacts in accordance with ISO 7816-2	15
2.8	Contact locations in relation to body of card	16
2.9	Cold reset sequence	20
3.1	ATR, PTS and first instruction sent to card	22
3.2	The OSI Reference Model	23
3.3	OSI communication model between terminal and Smart Card	24
3.4	(a) Illustration of error-free transmission of bytes with T=0 on the I/O channel (b) Illustration of	

	transmission error in T=0 due to a low level in the I/O interface during the guard time	27
3.5	Creating an instruction with T=0	28
3.6	Node address (NAD field)	33
3.7	Definition of character waiting time (CWT)	35
3.8	Definition of block waiting time (BWT)	37
3.9	Definition of block guard time (BGT)	38
3.10	PCB field I-block	39
3.11	PCB field in R-block	39
3.12	PCB field in S-block	40
3.13	Progress of waiting time extension	41
3.14	Time diagram of reset signal and ATR start in accordance with ISO/IEC 7816-3	43
3.15	Basic ATR structure	44
3.16	(a) Time diagram of initial character TS with direct convention (b) Time diagram of initial character TS with inverse convention	45
3.17	Initial character TS codes	45
3.18	Format character TO codes	46
3.19	TA1 codes	47
3.20	FI codes	47
3.21	DI codes	47
3.22	TB1 codes	48
3.23	TC1 codes	49
3.24	TB2 codes	49
3.25	TC2 codes	50

3.26	TAi (i>2) codes	50
3.27	TBi (i>2) codes	51
3.28	TCi (i>2) codes	51
3.29	TA2 codes	52
3.30	TDi byte codes	53
3.31	Basic PTS structure	54
3.32	PTS0 codes	55
3.33	PTS1 codes	55
3.34	PTS2 codes	55
3.35	Application communications architecture	56
3.36	Structure of an APDU command	57
3.37	Command APDU cases	58
3.38	Structure of response APDU	59
3.39	System of return codes in accordance with ISO/IEC 7816-4	59
4.1	Symmetric key encryption	62
4.2	Asymmetric key encryption	63
4.3	A digital signature using message digest	65
5.1	Life-cycle of a smart card	71
5.2	Silicon wafer with defective dice identified by a spot of paint	72
5.3	A single die is attached to a module	74
5.4	Wire bonding	74
5.5	Encapsulation by protective coat	75
5.6	Milling of module cavity	78
7.1	Pinout of the 8051 microcontroller	87

7.2	The block diagram of the 8051 microcontroller	88
7.3	The memory map of the 8051 internal RAM	93
7.4	The development cycle	95
7.5	Levels of software	96
7.6	Components of a microcontroller system	100
7.7	The CPU Subsystem	102
7.8	The Memory Block	104
7.9	The Input/Output Block	105

CHAPTER 1

INTRODUCTION

1.1 History

Around twenty years ago, French banks were facing fake credit card problem and suffered a great loss. Magnetic-stripe technology was the technology used for the credit cards at that time. Magnetic-stripe cards could be easily counterfeited and counterfeiting magnetic-stripe credit cards became widespread in France.

Also, the data stored on the stripe can be read, deleted and rewritten by anyone with appropriate read and write device. Hence, confidential data was not suitable stored on the stripe and most system employing magnetic stripe cards were connected on-line to the system's host computer. Deployment of transmission links to enable on-line transactions caused considerable costs to those banks using this magnetic stripe technology.

Due to these problems, French government, Cartes Bancaires (French banking association) and Bull CP8, a French computer company started working together to find a solution. In 1974, a French journalist Roland Moreno came out with a concept of having a microprocessor chip on a credit card to reduce counterfeiting. In March 1979, Bull CP8 successfully developed the first operational microprocessor card. The card had a memory chip and a microprocessor supplied by Motorola.

Emergence of smart cards had solved the fake credit card problem. Since smart cards have high degree security features, confidential data can be stored on the cards and off-line transaction is achieved. In 1993, this original application of smart cards had reached full implementation, when all banking cards in France were converted into smart cards.

Apart from being used in financial transaction, smart cards can be used in other applications. In 1982, the world's first large-scale use of smart cards was in Monte-Carlo during the European Financial Marketing Association (EFMA) congress. 500 smart cards were distributed to the delegates for they used these cards to pay their expense.

In 18 November 1983, the French Social Affairs Minister, Pierre Beregovoy announced the launch of two experimental operations to test the use of smart cards in health and social services sector. These experiments were carried out in Blois and involving 4500 children and the French hemodialysis population. The 4500 children used smart cards to keep their vaccination records whereas every French hemodialysis patient was given a smart card to facilitate their access to the 150 French dialysis centers.

In the same year, the first card payphones were installed in France by Schlumberger and were produced by Flonic Schlumberger for France Telecom.

Gradually, this new technology started grasping the world's attention. More and more players from different countries involved themselves to develop this technology. And also more and more applications using smart cards were found. Especially, when electronic components growing smaller in size, the demand of smart cards has grown rapidly.

At first, North America was not enthusiastic in this industry. It was due to North America had a well deployment of telecommunications links which

could enable on-line transactions. But, emergence of new markets such as using smart cards as a subscriber identification module (SIM) in the GSM digital mobile phone in 1990, has dragged North America into this new industry.

1.2 Smart Card

Smart cards, also known as "chip cards" or "integrated circuit cards" are cards with size of credit card which have an embedded silicon chip. This silicon chip is actually a microcontroller or microprocessor. It is this chip which makes smart cards smart and intelligent.

One of the important features of smart cards is their highly security features. Different technologies such as using personal identification number (PIN), applying complex cryptographic algorithms (DES, RSA) and biometrics are used to enhance the security of the data on the cards. All these can be done because of the microcontroller or microprocessor embedded on the cards. The central processing unit (CPU) in the chip can make decision, manipulate data and perform complex calculation. Powerful CPU is the centre core for applying all these security technologies.

Besides CPU, there are different types of memories on the chip. There are ROM, RAM and EEPROM. ROM and EEPROM are non-volatile memories whereas RAM is volatile memory. Non-volatile memory means that the data is still in the memory although the power is off. These memories make the smart cards have greater storage capacity – 10 times more than magnetic stripes. Another advantage of smart cards over the magnetic-stripe technology is that data can be written into the memory of the cards whereas data only can be read from the magnetic stripes.

ROM is used to store the operating system and cannot be changed. Its capacity usually ranges from 16 kB to 32 kB. EEPRO is used to store personal data like financial and medical data. Data in EEPROM can be always updated and modified. It is also used to store the application program and sometimes also part of the operating system. It can only be erased and reprogrammed 10,000 and 100,000 of times. It is usually range between 1 kB to 16 kB. RAM provides a scratchpad for calculation or manipulation of data. The data in RAM is lost when the power is off. RAM's capacity ranges from 256 bytes to 1 kB.

The capacity of these memories is depending on the type of the application. Also, some of the applications need a very powerful microprocessor. In general, applications of smart card can be categorized into two categories. First type is the memory card. Memory cards are primarily information storage cards that contain value which users can "spend" in a pay phone, retail, vending or related transaction. They can be subdivided into disposable card and reloadable card. The disposable card in thrown after the value is finished whereas reloadable card can be reloaded the value.

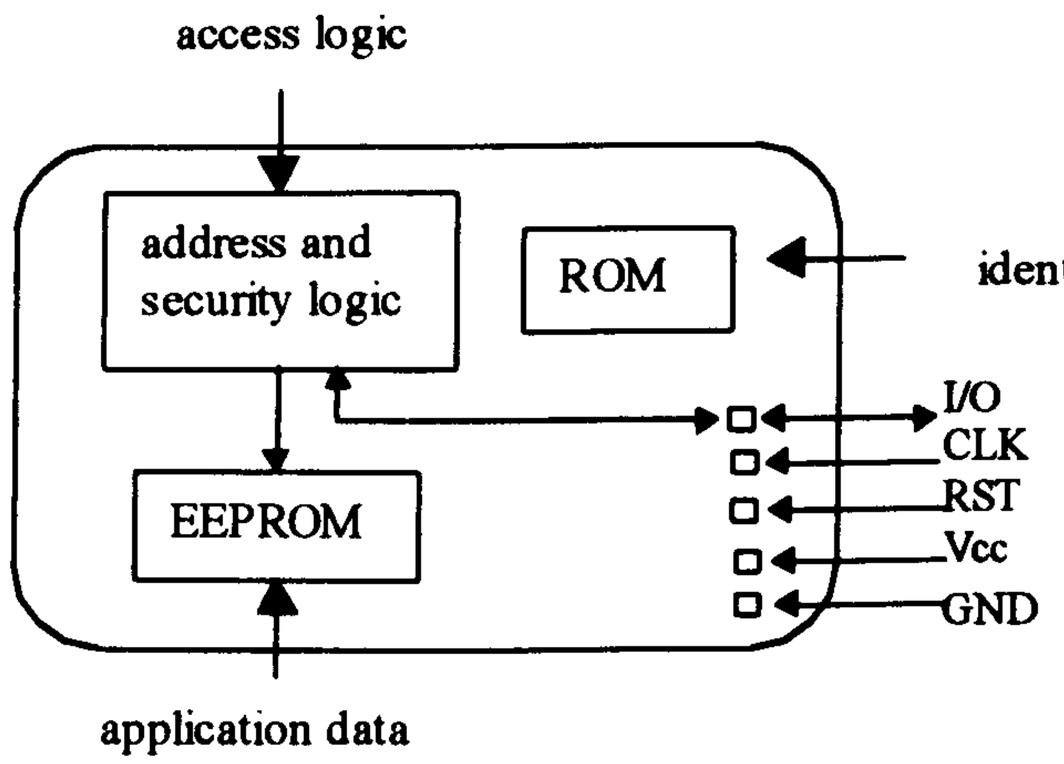

Figure 1.1 Typical architecture of a memory card with security logic.

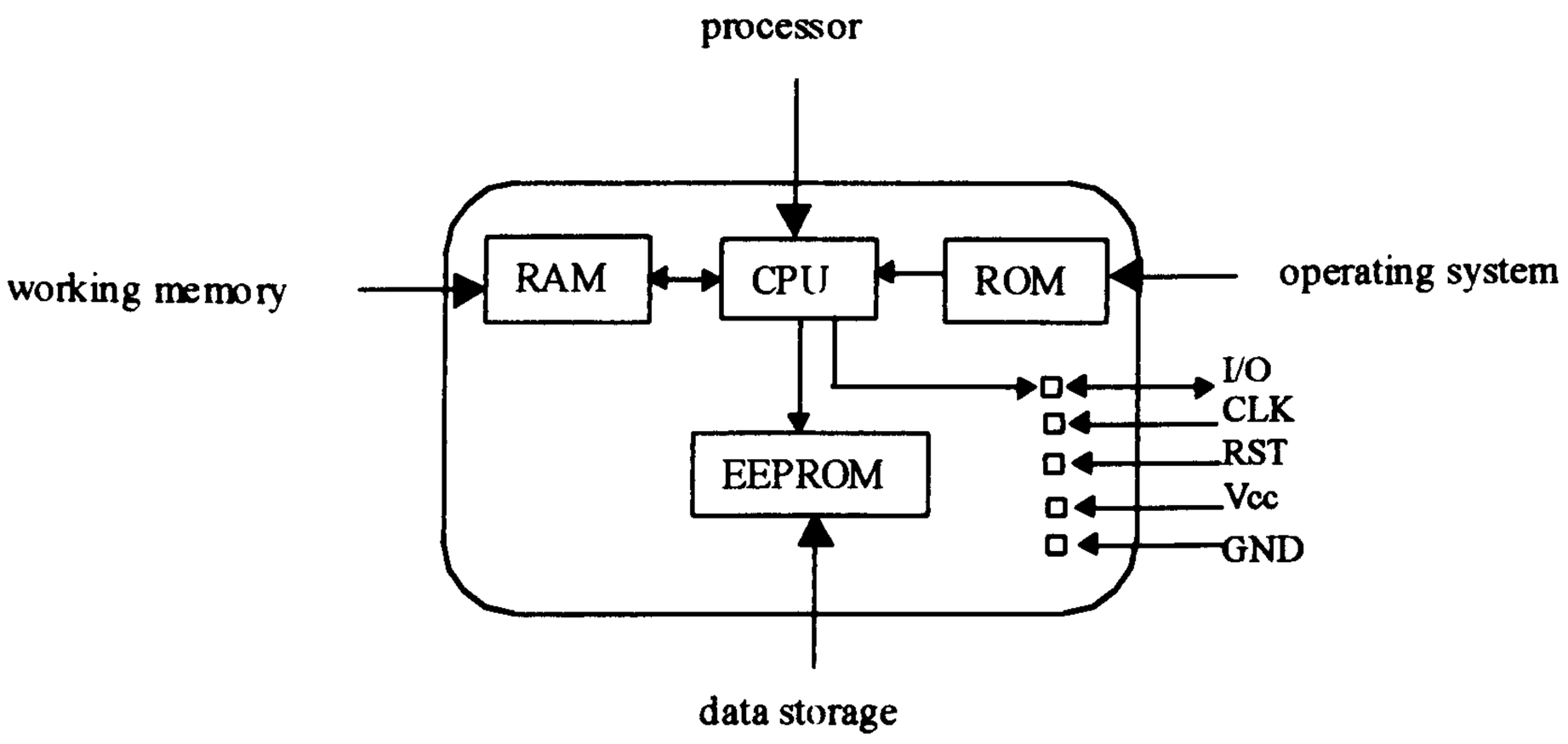

Figure 1.2 Typical architecture of microprocessor cards.

The second type is called intelligent card. This type of smart card includes a processor on the chip in addition to the memories. Sometimes, two processors are included for those applications which need high processing power. Intelligent cards are usually used in military applications and also applications which need high security features. For example, door-access card, bank card, personal ID card and other applications which need verification of the authorized users.

Microcontroller or microprocessor of a smart card has only five standard pinouts: I/O, clock, power, ground and reset, whereas other microcontrollers or microprocessors usually have at least 16 pins and sometimes more than 50. These pins are electrically connected to the golden contact plate seen on the smart cards. These contacts interfacing the smart cards with terminal or other interface devices. They are sometimes known as smart card readers. There must

be a mutually agreed protocol to let the terminal and the cards communicate. A terminal provides power for smart cards and also provides data for smart cards to manipulate through the contact plate.

Apart from these contact smart cards, there are contactless smart cards. These cards use radio frequency to communicate between the cards and the terminal. The power for the smart cards is also provided through this radio frequency. The advantage for contactless cards is that they do not need physical contact between the cards and the terminal. Thus, the transaction process can be very fast; sometimes even without the users to take out their smart cards from their wallets. But, of course this only limited to certain lengths between the cards and terminal.

In order for this technology to be widespread, compatibility with the existing technology like magnetic-stripe must be achieved. Hybrid cards are the cards not only embedded with microprocessor chip but also magnetic stripe and bar coding. Thus, different hardware systems, such as card readers, ATM machine and bar code applications can be accessed by these hybrid cards. Besides, cardholder's photograph, printed name and signature would further enhance the hybrid cards' already significant security features.