การประยุกต์ใช้สมาร์ตการ์ดกับระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์

Application for smart card with computer network voting system

โดย

นาย เจตนา หยงสตาร์

นาย สาโรจน์ พิจารณาธรรม

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตร์บัณฑิต

สาขาวิชาวิศวกรรมสารสนเทศ ภาควิชาวิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2544

APPLICATION FOR SMART CARD WITH COMPUTER NETWORK VOTING SYSTEM

Mr. JETTANA YONGSTAR

Mr. SAROJ PIJARANATAM

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF

THE REQUIREMENT FOR THE DEGREE OF

BACHELOR OF THE TECHNOLOGY TELECOMMUNICATIONS

FACULTY OF ENGINEERING

KING MONKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2001

หัวข้อปริญญานิพนธ์	การประยุกต์ใช้สมาร์ตการ์ดกับระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์ Application for smart card with computer network voting system
นักศึกษา	นาย เจตนา หยงสตาร์ เลขที่ประจำตัว 41014081 นาย สาโรจน์ พิจารณาธรรม เลขที่ประจำตัว 41014458
อาจารย์ที่ปรึกษา	กฤดากร กล่อมการ
ระดับการศึกษา	ปริญญาวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมสารสนเทศ
ภาควิชา	วิศวกรรมสารสนเทศ
ปีการศึกษา	2544

ปริญญานิพนธ์ฉบับนี้ได้รับความเห็นชอบจากอาจารย์ที่ปรึกษาเป็นที่เรียบร้อยแล้ว

กฤดากร

.....

(อาจารย์กฤดากร กล่อมการ)

อาจารย์ผู้ควบคุมวิทยานิพนธ์

หัวข้อปริญญานิพนธ์ การประยุกต์ใช้สมาร์ตการ์ดกับระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์
Application for smart card with computer network voting system

นักศึกษา นาย เจตนา หยงสตาร์ เลขที่ประจำตัว 41014081
นาย สาโรจน์ พิจารณาธรรม เลขที่ประจำตัว 41014458

อาจารย์ที่ปรึกษา กฤดากร กล่อมการ
ภาควิชา วิศวกรรมสารสนเทศ
ปีการศึกษา 2544

บทคัดย่อ

ปริญญานิพนธ์ฉบับนี้นำเสนอถึง การใช้บัตรสมาร์ตการ์ด (Smart Card) มาประยุกต์ใช้เป็นบัตรประจำตัวประชาชน ซึ่งใช้สำหรับบันทึกข้อมูลส่วนตัวของผู้ถือบัตร และนำมาประยุกต์ใช้กับระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์แทนวิธีการเลือกตั้งในปัจจุบัน โดยใช้เทคโนโลยีจาวาการ์ด (Java Card) และเทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure) มาสร้างระบบรักษาความปลอดภัยให้แก่ระบบเลือกตั้งดังกล่าว

Thesis Title	Application for smart card with computer network voting system	
Student	Mr. JETTANA	YONGSTAR ID 41014081
	Mr. SAROJ	PIJARANATAM ID 41014458
Advisor	Mr. KIDAKORN	KLOMKAN
Academic Year	2001	

ABSTRACT

This thesis presents applications for smart card with the nation identity card and electronic voting system. The java card technology and public key infrastructure are the system's tools for security environment in the electronic voting.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยดี ด้วยคำแนะนำและคำปรึกษาจาก อ.กฤดากร กล่อมการ ซึ่งเป็นอาจารย์ผู้ควบคุมปริญญานิพนธ์ ผู้จัดทำรู้สึกซาบซึ้งในความอนุเคราะห์จากท่าน และขอกราบขอบพระคุณอย่างสูง

ขอกราบขอบพระคุณ คุณพ่อ คุณแม่ ที่คอยห่วงใยและให้การสนับสนุนในการศึกษา รวมทั้งขอขอบคุณญาติสนิทและพี่ๆ ทุกคนที่เป็นกำลังใจพร้อมทั้งให้ความช่วยเหลือในด้านต่างๆโดยตลอด

ขอขอบคุณเพื่อน ๆ นักศึกษาทุกคนที่ช่วยเหลือให้คำแนะนำต่างๆ พร้อมทั้งช่วยตรวจเทียบและแก้ไขทฤษฎีและอื่น ๆ ที่ผิดพลาด จนสำเร็จสมบูรณ์ยิ่งขึ้นและยังให้กำลังใจแก่ผู้จัดทำอย่างใกล้ชิดตลอดมา

คุณค่าและประโยชน์อันพึงมีจากปริญญานิพนธ์ฉบับนี้ ผู้จัดทำขอมอบแด่ผู้มีพระคุณทุกท่าน

นาย เจตนา หยงสตาร์

นาย สาโรจน์ พิจารณาธรรม

ผู้จัดทำ

สารบัญ

สารบัญรูป

บทที่ 1
บทนำ

1.1 ความสำคัญและความเป็นมา

เนื่องจากในปัจจุบันโครงการรัฐบาลอิเล็กทรอนิกส์ (E-Government) ได้เข้ามามีบทบาทในระบบงานต่างๆ ของภาครัฐบาล เพื่ออำนวยความสะดวกในการติดต่อสื่อสารและการบริการแก่ประชาชน และหน่วยงานเอกชน ระบบงานหนึ่งที่รัฐบาลไทยมีแนวคิดที่จะพัฒนา คือ ระบบการทำบัตรประชาชนอิเล็กทรอนิกส์ โดยใช้บัตรสมาร์ตการ์ดแทนบัตรพลาสติกที่ใช้กันอยู่ในปัจจุบัน เพื่ออำนวยความสะดวกและความปลอดภัยในการทำธุระกรรมต่างๆ กับทางภาครัฐ โครงงานนี้จึงได้แนวคิดในการนำเอาบัตรสมาร์ตการ์ด มาประยุกต์ใช้เป็นบัตรประจำตัวประชาชนและพัฒนาให้สามารถใช้กับระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์ โดยคำนึงถึงความปลอดภัยของข้อมูลเป็นหลัก ซึ่งจะเป็นพื้นฐานต่อการพัฒนาไปสู่ระบบการเลือกตั้งอิเล็กทรอนิกส์ ของประเทศไทยในอนาคต

1.2 วัตถุประสงค์ของการวิจัย

ผู้จัดทำได้เล็งเห็นถึงความสำคัญของเทคโนโลยีรักษาความปลอดภัยคอมพิวเตอร์ และความสำคัญของเทคโนโลยีสมาร์ตการ์ด ที่จะเข้ามามีบทบาทอย่างใกล้ชิดในชีวิตประจำวันของเราในระยะเวลาอันใกล้นี้ เช่น ระบบบัตรประชาชนอิเล็กทรอนิกส์ ระบบเลือกตั้งอิเล็กทรอนิกส์ ทางผู้จัดทำจึงได้ทำการรวบรวมข้อมูลต่างๆ แล้วนำมาออกแบบระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์ ซึ่งวัตถุประสงค์หลักดังต่อไปนี้

1. เพื่อเป็นการนำเสนอทั้งภาคทฤษฎีและปฏิบัติในการสร้างระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์ โดยคำนึงถึงด้านความปลอดภัยของข้อมูลเป็นหลัก
2. เพื่อให้รู้แนวโน้มและเกิดแนวคิด เกี่ยวกับระบบการเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์ แล้วนำมาประยุกต์ใช้ในอนาคต
3. เพื่อสนับสนุนแนวคิดรัฐบาลอิเล็กทรอนิกส์ ที่จะเข้ามามีบทบาทต่อชีวิตประจำวันของประชาชนในอนาคตอย่างหลีกเลี่ยงไม่ได้

1.3 ขอบเขตของงานวิจัย

โครงงานนี้มีวัตถุประสงค์ที่จะศึกษาวิจัยระบบรักษาความปลอดภัยในเครือข่ายคอมพิวเตอร์ โดยการนำเอาสมาร์ตการ์ดมาประยุกต์ใช้เป็นบัตรประจำตัวประชาชน แล้วนำมาใช้กับระบบเลือกตั้ง

ผ่านเครือข่ายคอมพิวเตอร์ ซึ่งโครงงานนี้แบ่งระบบการทำงานเป็น 2 ระบบ คือ ระบบงานทะเบียนและการออกบัตร และ ระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์

ระบบแรกเป็นขั้นตอนการออกบัตรประชาชนให้แก่ผู้ขอมีบัตรประจำตัวเป็นครั้งแรก หรือผู้ที่ทำบัตรใหม่ เมื่อบัตรเดิมหมดอายุหรือเกิดการสูญหาย ส่วนระบบที่สองเป็นบริการที่นำเอาบัตรประชาชนอิเล็กทรอนิกส์ที่ได้จากระบบแรก มาประยุกต์ใช้กับระบบรักษาความปลอดภัยคอมพิวเตอร์ เพื่อใช้ในการเลือกตั้งอิเล็กทรอนิกส์

1.4 คุณสมบัติและความสามารถของระบบ

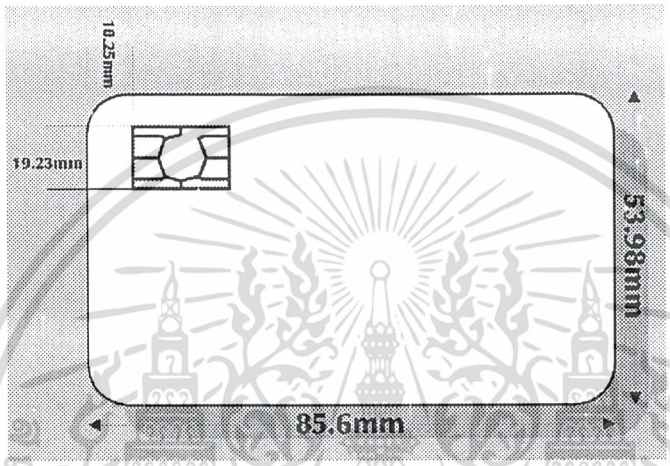
1. สามารถทำการออกบัตรประจำตัวประชาชนให้แก่ผู้ทำบัตรเป็นครั้งแรก และผู้ที่ต้องการเปลี่ยนบัตรประจำตัว เมื่อบัตรใบเก่าหมดอายุ
2. สามารถทำการออกบัตรประจำตัวประชาชนให้แก่ผู้ที่ทำบัตรประชาชนหาย หรือผู้ที่ต้องการแก้ไขข้อมูลส่วนตัว
3. สามารถทำการตรวจสอบ และรับรองรายการบัตรประจำตัวประชาชน
4. สามารถทำการเปลี่ยนรหัส PIN ของบัตรประจำตัวประชาชน
5. สามารถทำการปลดล็อครหัส PIN แก่บัตรที่ถูกล็อค
6. สามารถนำบัตรประจำตัวประชาชน ไปใช้บริการอื่น ๆ ของทางภาครัฐได้
7. สามารถให้บริการต่าง ๆ ดังที่กล่าวมาแล้ว ที่สำนักทะเบียนทุกแห่ง

1.5 ผลที่คาดว่าจะได้รับ

- ลดการใช้เอกสาร แบบพิมพ์ และสถานที่จัดเก็บ
- กระจายอำนาจ และลดขั้นตอนการปฏิบัติงาน
- บริการแบบเบ็ดเสร็จและรวดเร็ว ณ สำนักทะเบียน
- รักษาความถูกต้องและป้องกันความผิดพลาดของรายการทะเบียน
- สร้างความมั่นคงและถาวรของรายการทะเบียน
- ให้หน่วยงานต่าง ๆ ตรวจสอบรายการทะเบียนได้จากระยะไกล
- เชื่อมโยงข้อมูลรายการทะเบียนที่จำเป็นของหน่วยงานต่าง ๆ เพื่อใช้ประโยชน์ร่วมกัน เพื่อลดค่าใช้จ่ายและสร้างบริการแบบ One Stop Service
- สร้างบัตรประชาชนใบเดียวใช้งานได้ หลายบริการ หลายหน่วยงาน
- จัดทำข้อมูลสถิติทางด้านประชากรในรูปแบบต่าง ๆ เพื่อสนับสนุนการวิจัยและวางแผนพัฒนาประเทศภาครัฐและพัฒนาธุรกิจภาคเอกชน

บทที่ 2
ทฤษฎีที่เกี่ยวข้องกับโครงงาน

2.1 ลักษณะของสมาร์ตการ์ด



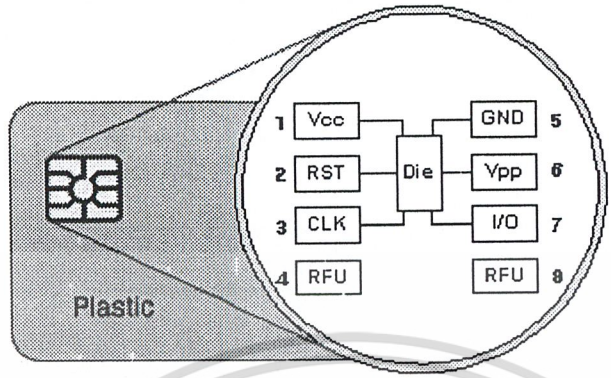
รูปที่ 2.1 แสดงลักษณะและขนาดของสมาร์ตการ์ด

สมาร์ตการ์ดมักถูกเรียกบ่อยๆว่าชิบการ์ด (Chip Card) หรือ ไอซีการ์ด (IC Card) มีขนาดเท่ากับบัตรเครดิต ภายในบรรจุวงจรอิเล็กทรอนิคส์ที่ใช้ในการรับส่ง, เก็บ และประมวลผลข้อมูล ลักษณะทางกายภาพและคุณสมบัติต่างๆ ของตัวสมาร์ตการ์ด กำหนดในมาตรฐาน ISO

2.2 ส่วนประกอบของสมาร์ตการ์ด

สมาร์ตการ์ดใช้หน้าสัมผัสซึ่งอยู่บนพื้นผิวพลาสติก , หน่วยประมวลผลกลางที่ฝังอยู่ภายในและชนิดหน่วยความจำหลายๆแบบ บางชนิดก็มีหน่วยประมวลผลร่วมที่ใช้ในการช่วยประมวลผลทางด้านคณิตศาสตร์

2.2.1 Smart Card Contact Points



รูปที่ 2.2 แสดง Smart Card Contact Points

2.2.2 Smart Card Central Processing Unit

หน่วยประมวลผลกลางที่ใช้เป็นส่วนใหญ่ในปัจจุบันเป็นไมโครคอนโทรลเลอร์ชนิด 8 บิต ใช้ชุดคำสั่ง Motorola 6805 หรือ Intel 8051 และความเร็วสัญญาณนาฬิกาถึง 5 MHz การ์ดรุ่นที่มีราคาแพงจะมีสัญญาณนาฬิกาความเร็ว 40 MHz (5 MHz * 8)

การ์ดรุ่นใหม่ๆมีไมโครคอนโทรลเลอร์ชนิด 16 บิต หรือ 32 บิต และได้ใช้สถาปัตยกรรม RISC (Reduce Instruction Set)

2.2.3 Smart Card Coprocessors

สมาร์ตการ์ดถูกออกแบบเพื่อใช้ในการที่ต้องการระบบความปลอดภัยมักจะมีการฝัง หน่วยประมวลผลร่วมไว้ภายในตัวการ์ด หน่วยประมวลผลร่วมเป็นวงจรพิเศษที่ช่วยเพิ่มความเร็วในการคำนวณ, การประมวลผลฟังก์ชั่นที่มีความซับซ้อน เช่นการคำนวณอัลกอริทึมเข้ารหัส RSA

2.2.4 Smart Card Memory System

โดยทั่วไปสมาร์ตการ์ดบรรจุหน่วยความจำไว้ 3 ชนิดคือ Persistent Non-Mutable Memory, Persistent Mutable Memory และ Non-Persistent Mutable Memory หรือ ROM, EEPROM และ RAM ตามลำดับ

2.3 การติดต่อสื่อสารของสมาร์ตการ์ด

2.3.1 Card Acceptance Device

เครื่องอ่านบัตรติดต่อคอมพิวเตอร์ผ่านทาง Serial, Parallel หรือ USB พอร์ท เครื่องอ่านบัตรมีช่องสำหรับเสียบบัตรหรือเป็นช่องสำหรับรับข้อมูลแม่เหล็กไฟฟ้าในกรณีเป็นแบบ Contactless Card

2.3.2 Smart Card Communication Model

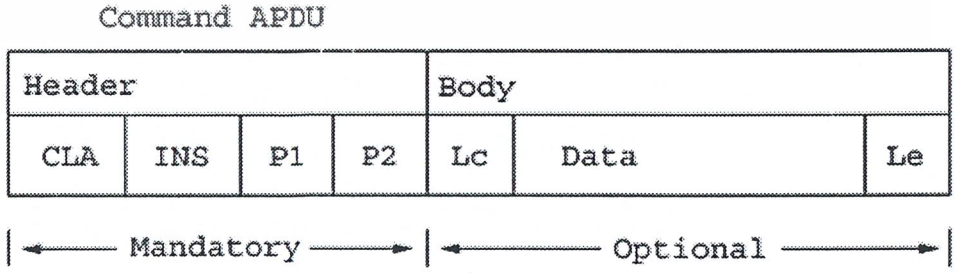
วิธีการติดต่อระหว่างบัตรและคอมพิวเตอร์เป็นแบบกึ่ง Duplex ซึ่งข้อมูลสามารถถูกส่งหรือรับได้อย่างใดอย่างหนึ่งในเวลาเดียวกันเท่านั้น

เมื่อคอมพิวเตอร์ติดต่อซึ่งกันและกัน การแลกเปลี่ยนข้อมูลใช้รูปแบบการสื่อสารดังเช่น TCP/IP ส่วน สมาร์ตการ์ดรับส่งข้อมูลไปสู่คอมพิวเตอร์ด้วยแพกเกจข้อมูลชนิดหนึ่งที่เรียกว่า APDUs (Application Protocol Data Units) ซึ่ง บรรจุคำสั่งหรือข้อมูลตอบสนองอย่างใดอย่างหนึ่ง

ในการทำงานเป็นโมเดลลักษณะ Master-slave คือ สมาร์ตการ์ดทำหน้าที่ Passive (slave) รอคำสั่ง APDU จากคอมพิวเตอร์ จากนั้นทำการปฏิบัติการตามคำสั่งที่กำหนดไว้และส่งข้อมูลตอบรับ APDU สู่คอมพิวเตอร์

2.3.3 APDU Protocol

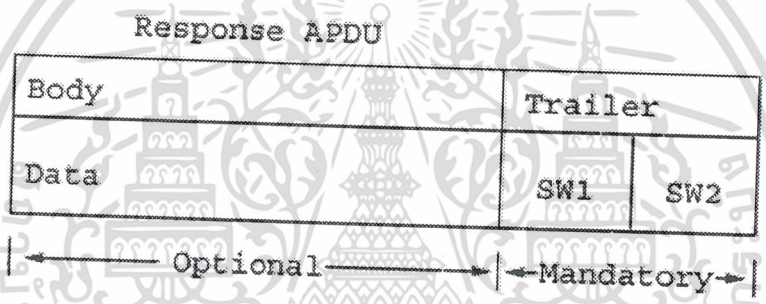
โปรโตคอล APDU ที่กำหนดไว้ใน ISO 7816-4 เป็น Application Level Protocol ระหว่างสมาร์ตการ์ดและคอมพิวเตอร์ APDU ภายใต้ ISO 7816-4 ประกอบด้วยโครงสร้าง 2 อย่าง Command APDU (C-APDU) และ Response APDU (R-APDU)



รูปที่ 2.3 แสดง Format ของ Command APDU

Command APDU Header ประกอบด้วย 4 ไบต์คือ CLA (Class of Instruction), INS (Instruction Code) , P1 และP2 (Parameter 1 และ 2) Class byte เป็นตัวกำหนดประเภทของ Command หรือ Response APDU ส่วน Instruction byte กำหนดคำสั่งของ Command ส่วน Parameter byte P1 และ P2 ใช้สำหรับรายละเอียดปลีกย่อย

ส่วนถัดมาคือ Header ใน Command APDU ประกอบไปด้วย Lc Field เป็นตัวกำหนดความยาวของข้อมูลในหน่วยไบต์ ส่วน Data Field บรรจุข้อมูลซึ่งถูกส่งให้ทำคำสั่งตามคำสั่งที่กำหนดไว้ใน Header ส่วนสุดท้ายคือ Le Field ซึ่งกำหนดจำนวนไบต์ที่คาดหวังว่าจะได้ตอบรับกลับมาจากโฮส



รูปที่ 2.4 แสดง format ของ Response APDU

Response APDU ถูกส่งจากการ์ดเพื่อเป็นการตอบกลับ Command APDU ประกอบไปด้วย Optional Body และ Mandatory Trailer ส่วน Body ประกอบด้วย Data Field ซึ่งความยาวเท่ากับที่ Command APDU ร้องขอมาตาม Le Field ส่วน trailer ประกอบด้วย SW1 และ SW2 เรียกว่า Status Word กำหนด state หลังจากที่ปฏิบัติคำสั่ง command APDU เสร็จแล้ว เช่น " 0x9000 " หมายความว่าคำสั่งได้ถูกปฏิบัติอย่างเรียบร้อยและสมบูรณ์ไม่มีข้อผิดพลาด

2.3.4 TPDU Protocol

APDU ถูกส่งโดยใช้ Transport Protocol ซึ่งกำหนดไว้ใน ISO 7816-3 โครงสร้างของข้อมูลถูกแลกเปลี่ยนระหว่างโฮสและการ์ดด้วย Transport Protocol จึงเรียกว่า Transmission Protocol Data Units หรือ TPDUs

Transport Protocol ที่ใช้ในระบบสมาร์ตการ์ด คือ T=0 Protocol และ T=1 Protocol T=0 protocol ส่งข้อมูลแบบ Single Byte คือส่งข้อมูลเป็นไบต์ต่อไบต์ ส่วน T=1 Protocol ส่งข้อมูลเป็น Sequence คือส่งเป็นบล็อกข้อมูลที่ประกอบไปด้วยหลายๆไบต์

2.3.5 ATR

ทันทีที่หลังจากเปิดสวิทซ์เข้ามาสมาร์ตการ์ดส่ง ATR (Answer To Reset) ไปสู่โฮส ATR สามารถยาวได้ถึง 33 ไบต์ ซึ่งบรรจุ Parameter เกี่ยวกับ Transmission ต่างๆ เช่น Transport Protocol, Data Transmission Rate , Card Hardware Parameter เช่น Chip Serial Number และ Mask Version Number และข้อมูลอื่นๆเกี่ยวกับการ์ดที่โฮสต้องการรู้

2.4 เทคโนโลยีจาวาการ์ด

2.4.1 Architecture Overview

สมาร์ตการ์ดได้รับการยอมรับว่าเป็นหนึ่งในหน่วยคอมพิวเตอร์ที่เล็กที่สุดที่ใช้กันในทุกวันนี้ ค่าของหน่วยความที่ใช้กันมีดังต่อไปนี้ RAM 1K, EEPROM 16K และROM 24K สิ่งที่ท้าทายนักวิจัย Java Card Technology คือการออกแบบให้ซอฟท์แวร์ทำงานได้ดี ในสภาวะที่ใช้เนื้อที่หน่วยความจำน้อยที่สุด การที่คำสั่งใน Java Card เป็นส่วนย่อยของภาษาจาวา ทำให้ประหยัดเนื้อที่หน่วยความจำ และยังแยกโมเดลของ Java Virtual Machine ออกมาทำงานอีกต่างหาก

Java Card Virtual Machine แบ่งเป็น 2 ส่วน คือ ส่วนที่ทำงานแบบ off-card (ทำงานโดยใช้โปรแกรมจำลองสภาพแวดล้อมขึ้นมา) และ on-card (ทำงานบนสภาวะแวดล้อมบนการ์ดจริงๆ)

ลักษณะที่สำคัญของ Java Card Runtime Environment คือ การแยกส่วนกันอย่างชัดเจนระหว่างระบบกับตัวแอพพลิเคชั่น แอพพลิเคชั่นต้องการภาษาระดับสูงในการพัฒนา

ดังนั้น Java Card Technology ได้กำหนดรูปแบบในการพัฒนาแอพพลิเคชั่นซึ่งเขียนด้วยภาษาจาวา สามารถทำงานบนสมาร์ตการ์ดและอุปกรณ์ต่อพ่วงได้ แอพพลิเคชั่นที่เราเขียนขึ้นเรียกว่า Applet ประกอบไปด้วยมาตรฐาน 3 ส่วนคือ

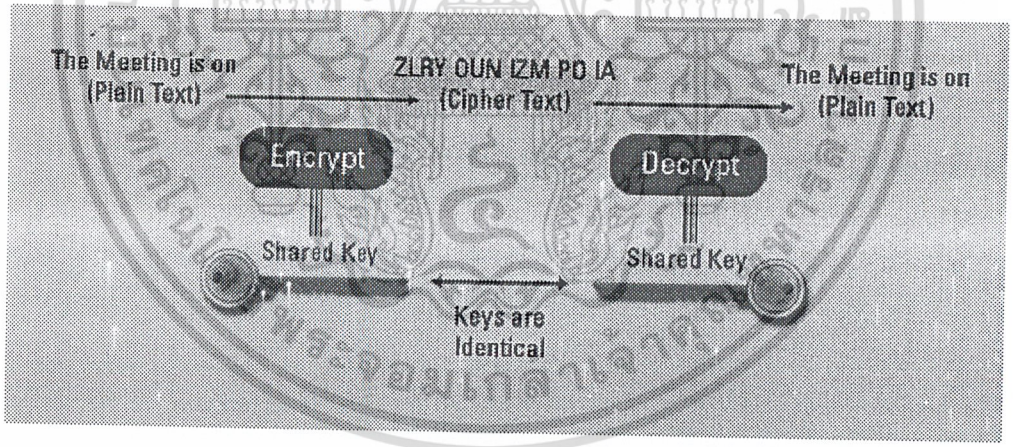
- The Java Card Virtual Machine (JCVM)
- The Java Card Runtime Environment (JCRE)
- The Java Card Application Programming Interface (API)

2.5 ระบบรักษาความปลอดภัยโดยใช้ Public Key Infrastructures

Algorithm ที่ใช้ในการเข้ารหัสข้อมูลมีจำนวนมากมาย ซึ่งในอดีตที่ผ่านมานั้น การเข้ารหัสและการถอดรหัสข้อมูลจะกระทำโดยใช้กุญแจตัวเดียวกัน ซึ่งถูกเรียกว่ากุญแจสมมาตร แต่กว่า 20 ปีที่ผ่านมานี้ เครื่องมือในการเข้ารหัสและถอดรหัสได้ถูกคิดค้นและพัฒนากุญแจขึ้นมาใหม่ ซึ่งเรียกว่ากุญแจไม่สมมาตรโดยจะใช้กุญแจคนละตัวกันในการเข้ารหัสและถอดรหัสข้อมูล ซึ่งกุญแจทั้งสองประเภทนี้ก็จะมีทั้งจุดแข็งและจุดอ่อนแตกต่างกันออกไป ในการใช้งานจริง จึงมีการนำเอาจุดแข็งของกุญแจทั้งสองประเภทมาประกอบกันเป็นเทคโนโลยี Public Key Infrastructure หรือ PKI ซึ่งภายใต้ขอบเขตการทำงานของ PKI เราจะสามารถทำการรักษาคุณสมบัติของระบบรักษาความปลอดภัยได้ทุกคุณสมบัติดังต่อไปนี้

2.5.1 Privacy

สามารถใช้ประโยชน์ได้จากกุญแจประเภทไม่สมมาตร โดยการใช้กุญแจเพียงกุญแจเดียวในการเข้ารหัสและการถอดรหัสข้อมูล เพราะกุญแจประเภทนี้จะสามารถประมวลผลได้อย่างรวดเร็ว จึงสามารถทำการเข้ารหัสและถอดรหัสได้ในแบบ Real-Time ผ่านทางระบบเครือข่าย

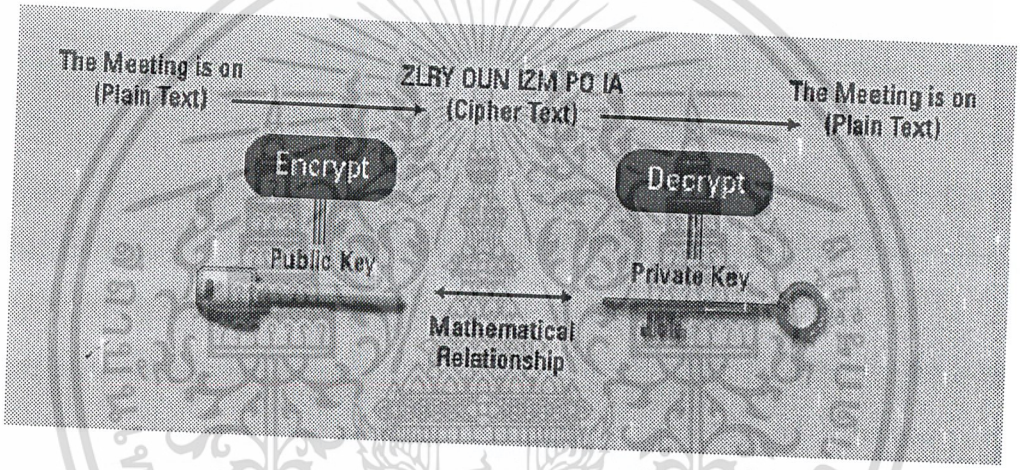


รูปที่ 2.5 แสดง Symmetric Encryption

2.5.2 Authentication

การรับรองความเป็นตัวตนสามารถทำได้โดยการใช้กุญแจประเภท กุญแจไม่สมมาตรในการเข้ารหัสและถอดรหัสข้อมูล ซึ่งจะต้องใช้การประมวลผลที่มีความซับซ้อนมาก แต่สามารถรักษาคุณสมบัติของโครงสร้างพื้นฐานในระบบรักษาความปลอดภัยในระบบที่มีขนาดใหญ่ได้ดีกว่า โดย

กุญแจหนึ่งจะทำหน้าที่ในการเข้ารหัสข้อมูล และอีกกุญแจจะใช้สำหรับการถอดรหัส การจัดการกุญแจจะจัดการ โดยกำหนดให้กุญแจตัวหนึ่งเป็นกุญแจสาธารณะ (Public Key) ซึ่งเป็นกุญแจที่สามารถแจกจ่ายไปให้แก่ผู้อื่นและเป็นตัวที่สามารถบอกความเป็นตัวตนของเจ้าของกุญแจได้ และอีกกุญแจหนึ่งเป็นกุญแจส่วนตัว (Private Key) ซึ่งทำหน้าที่เสมือนกุญแจลับ สำหรับวิธีการรับรองความเป็นตัวตนของกุญแจประเภทนี้ เริ่มจาก การใช้กุญแจสาธารณะทำการการเข้ารหัสข้อมูล ซึ่งจะทำให้มั่นใจได้ว่า เฉพาะบุคคลที่เป็นเจ้าของกุญแจส่วนตัว ซึ่งเป็นกุญแจที่คู่กันกับกุญแจสาธารณะเท่านั้น ที่จะถอดรหัสข้อมูลนั้นออกมาได้ จึงเป็นการรับรองและการยืนยันข้อมูลสองประการคือ ประการแรก บุคคลสามารถทำการเรียกร้องให้รับรองตัวตนของตนเองได้ และประการที่สอง เป็นการยืนยันได้ว่าคนที่มีกุญแจส่วนตัวที่ถูกต้องเท่านั้น ที่จะสามารถถอดรหัสข้อมูลได้



รูปที่ 2.6 Asymmetric Encryption

2.5.3 Authorization

การมอบอำนาจสิทธิสามารถทำได้ผ่านเครื่องมือดังต่อไปนี้ คือ Access Control List (ACL) หรือ ผ่านทางใบรับรองดิจิตอล (Digital Certificate) ในการใช้ ACL จะมีการมอบอำนาจ ณ จุดที่รับบริการ ซึ่งเป็นจุดที่ผู้ใช้สามารถเข้าถึงข้อมูลหรือบริการภายในระบบเครือข่าย ถ้าจะเปรียบเทียบการทำงานระหว่าง Web Browser กับ Web Server, ACL จะทำงานอยู่บน Web Server โดยเฉพาะการบริหารการอนุญาตและการให้อำนาจสิทธิตัวบุคคล ที่มีความสัมพันธ์กันกับ Server นั้น ยกตัวอย่าง เช่น ผู้ใช้ A สามารถทำการอ่านไฟล์ที่กำหนดได้ ส่วนผู้ใช้ B สามารถทำการอ่านและแก้ไขไฟล์นั้นได้ด้วย เป็นต้น อีกวิธีการหนึ่งก็คือ การบริหารอำนาจการให้สิทธิจากศูนย์กลางภายใต้เทคโนโลยี PKI โดยส่วนที่ทำหน้าที่ในการรับรองความเป็นตัวตนจะทำการให้สิทธิแก่ผู้ใช้จากศูนย์กลาง แล้วทำการกระจายไปสู่ Server ต่างๆ ในระบบเครือข่ายผ่านทางใบรับรองดิจิตอล (Digital Certificate) ซึ่งจะออกโดยหน่วยงานที่มีความน่าเชื่อถือ แล้วจึงส่งผ่านไปให้แก่ Information Server เพื่อทำการ

ตรวจสอบว่าใบรับรองดิจิตอลนั้นออกให้โดยหน่วยงานที่น่าเชื่อถือหรือไม่ และทำการตรวจสอบว่าข้อมูลที่ส่งมานั้น ไม่ได้รับการแก้ไขเปลี่ยนแปลงระหว่างการส่ง สิ่งแตกต่างที่ชัดเจนที่สุดระหว่างเครื่องมือสองชนิดนี้จุดที่เกิดการได้รับการอนุญาตจะถูกจัดการแตกต่างกัน

2.5.4 Information Integrity

ความสมบูรณ์ของข้อมูลถูกจัดการอยู่ภายใต้เทคโนโลยี PKI ผ่านเครื่องมือที่เรียกว่า ซองจดหมายดิจิตอล (Digital Envelope) ซึ่งใช้ Algorithm ที่เรียกว่า Message Authentication Code – MAC โดยใช้ในการประมวลผลข้อมูล ผลของการประมวลผลทำให้เกิดข้อมูลที่เรียกว่า Hash Code ซึ่งทั้งฟังก์ชัน MAC และ Hash Code จะทำหน้าที่เป็น Digital Envelope ยกตัวอย่างการทำงาน เช่น ถ้าผู้ใช้ A ทำการส่งข้อมูลไปยังผู้ใช้ B พร้อมกับการส่ง Hash Code ที่ผู้ใช้ A เป็นผู้ที่สร้างขึ้นมาโดยใช้ฟังก์ชัน MAC ไปด้วย ผู้ใช้ B จะสามารถตรวจสอบความถูกต้องของข้อมูลได้ด้วยการนำข้อมูลที่ได้รับมาทำการประมวลผลตาม Algorithm ของ MAC ถ้าผลที่ได้ตรงกันกับ Hash Code ก็จะสามารถมั่นใจได้ว่า ข้อมูลที่ส่งมานั้นไม่ได้รับการเปลี่ยนแปลงระหว่างการส่ง และโดยปรกติแล้วเพื่อเป็นการเพิ่มการรักษาความปลอดภัย จะทำการเข้ารหัส Hash Code ด้วยกุญแจส่วนตัวของผู้ส่ง เพื่อเป็นการรับประกันว่า Hash Code ที่ส่งมาด้วยนั้นไม่สามารถมีบุคคลใดสามารถเปิดอ่านได้ และเป็นการยืนยันได้ว่าผู้ส่งเป็นบุคคลที่ถูกต้อง

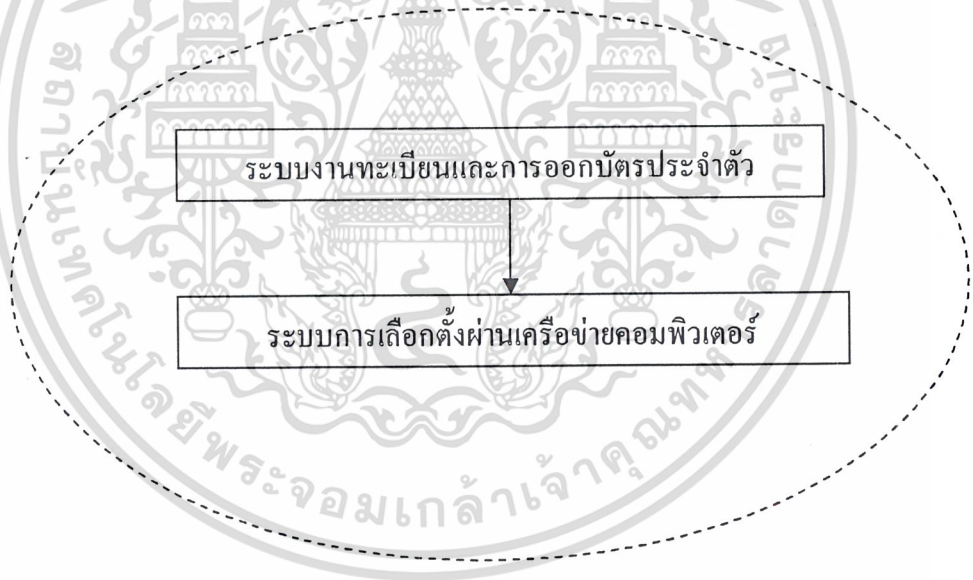
2.5.5 Non Repudiation

เป็นการทำงานภายใต้เทคโนโลยี PKI โดยการนำเอาลักษณะเฉพาะของโครงสร้างพื้นฐานข้ออื่นมาประกอบกัน คือ การรับรองความเป็นตัวตน และกระบวนการสร้างความถูกต้องสมบูรณ์ให้แก่ข้อมูลเข้า โดยเฉพาะข้อมูลที่ใช้ในการแลกเปลี่ยนสื่อสารกันระหว่างการทำธุรกรรมอิเล็กทรอนิกส์ ในรูปแบบของ Digital Envelope นอกจากนั้นแล้วยังต้องทำการเข้ารหัส Hash Code ด้วยกุญแจส่วนตัวของผู้ส่งด้วย วิธีการเข้ารหัส Hash Code นี้จะเรียกว่าลายเซ็นดิจิตอล (Digital Signature) ผู้ที่ทำการส่งข้อมูลสามารถทำการ sign ข้อมูลนั้นด้วยกุญแจส่วนตัวของตนเอง ซึ่งเป็นกุญแจลับสำหรับบุคคลอื่น และทางฝั่งผู้รับข้อมูลก็จะใช้กุญแจสาธารณะของบุคคลที่ส่งมานั้นทำการถอดรหัสจนได้ Hash Code และทำการ MAC ข้อมูลที่รับได้ แล้วทำการเปรียบเทียบ Hash Code ทั้งสอง ถ้า Hash Code ทั้งสองตรงกัน ผู้รับก็จะมั่นใจได้ว่าข้อมูลที่ส่งมานั้น มาจากผู้ส่งที่ถูกรับรองความมีตัวตนจริงๆ และผู้ส่งก็จะไม่สามารถปฏิเสธการทำธุรกรรมนั้นได้

บทที่ 3
การออกแบบและขั้นตอนการทำงาน

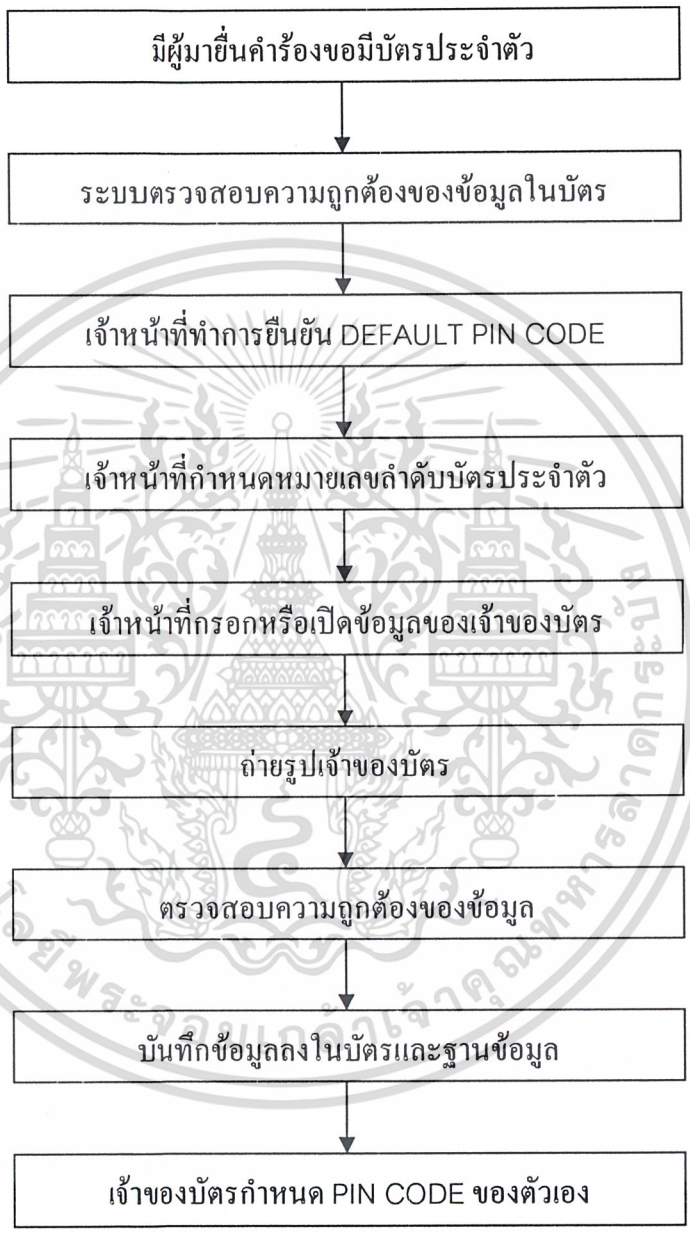
3.1 ขั้นตอนการทำงานของระบบ

โครงงานนี้เป็นการนำเอาสมาร์ตการ์ดมาประยุกต์ใช้เป็นบัตรประจำตัวประชาชน แล้วนำมาใช้กับระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์ ซึ่งโครงงานนี้แบ่งระบบการทำงานเป็น 2 ระบบ คือ ระบบงานทะเบียนและการออกบัตรประจำตัวประชาชน และ ระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์



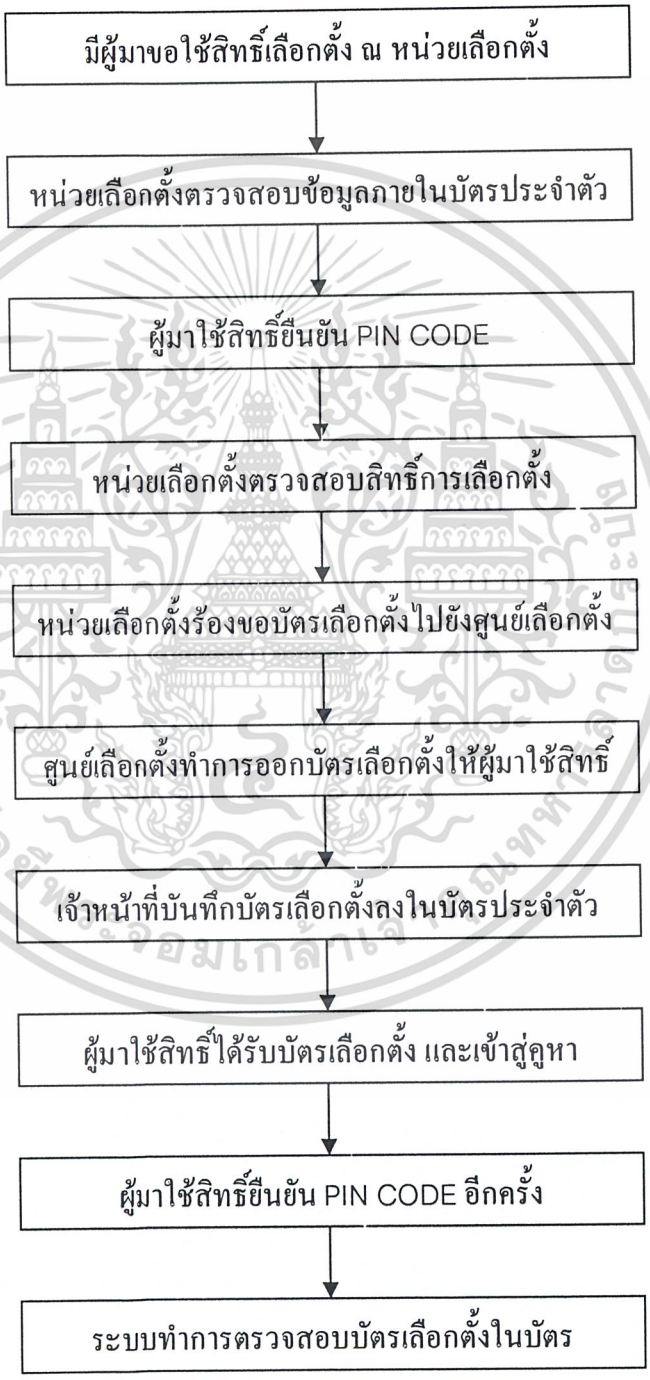
รูปที่ 3.1 แสดงขอบเขตการทำงานของระบบ

- ระบบงานทะเบียนและการออกบัตรประจำตัวประชาชน

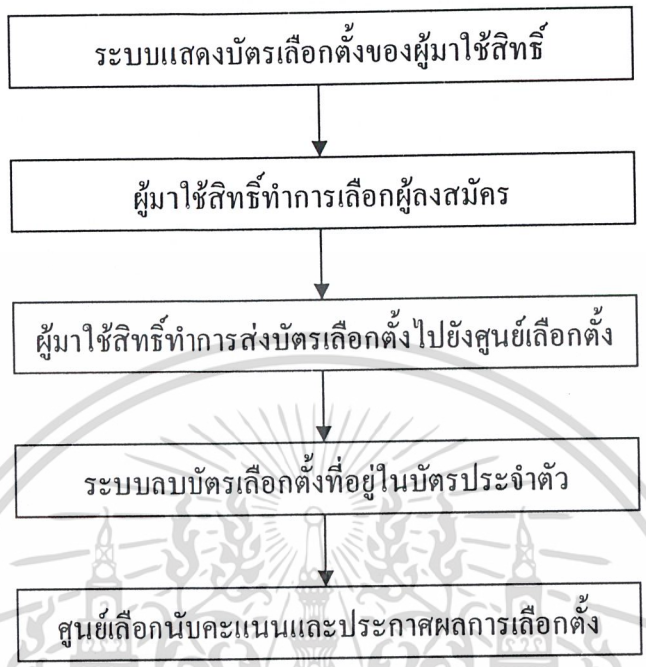


รูปที่ 3.2 แสดงขั้นตอนการออกบัตรประจำตัวประชาชน

- ระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์



รูปที่ 3.3 แสดงขั้นตอนการเลือกตั้ง

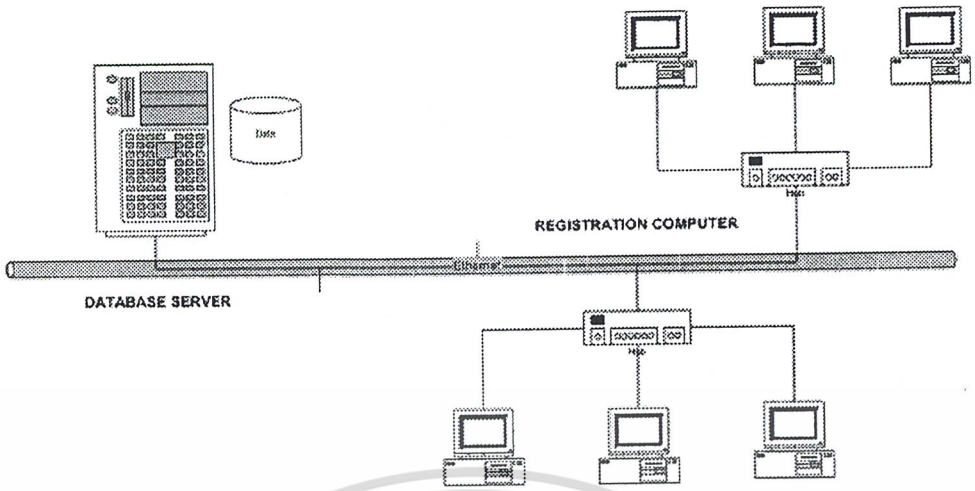


รูปที่ 3.3 แสดงขั้นตอนการเลือกตั้ง (ต่อ)

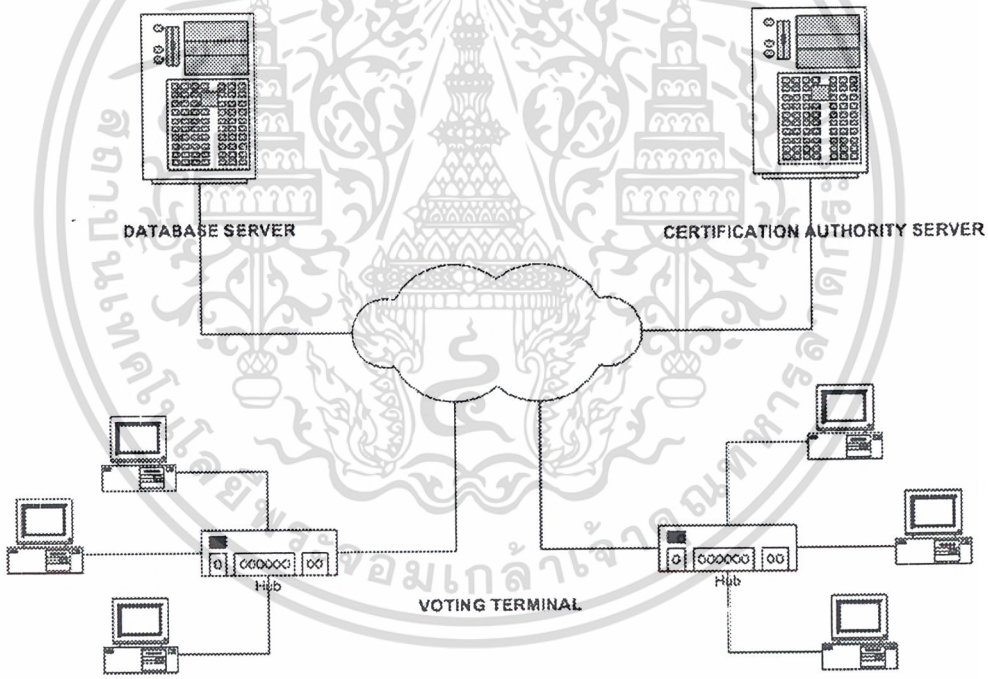
3.2 Network Diagram

อุปกรณ์ในเครือข่ายประกอบด้วยดังต่อไปนี้

- เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นเครื่อง Certification Authority Server ทำหน้าที่ออกใบรับรองให้แก่ผู้ใช้
- เครื่องคอมพิวเตอร์ Database Server ที่ทำหน้าที่เก็บฐานข้อมูลของบัตรประชาชน
- เครื่องคอมพิวเตอร์ Database Server ที่ทำหน้าที่เก็บฐานข้อมูลของการเลือกตั้ง
- เครื่องคอมพิวเตอร์ Client ของที่ใช้ทำหรือต่ออายุบัตรประชาชนในฝ่ายทะเบียน
- เครื่องคอมพิวเตอร์ Client ซึ่งใช้สำหรับการเลือกตั้ง
- เครื่องเขียน-อ่าน บัตรสมาร์ตการ์ด
- บัตรสมาร์ตการ์ดซึ่งใช้แทนบัตรประจำตัวประชาชนและใช้เก็บบัตรเลือกตั้ง



รูปที่ 3.4 โครงสร้างระบบเครือข่ายคอมพิวเตอร์สำหรับงานทะเบียน



รูปที่ 3.5 โครงสร้างระบบเครือข่ายคอมพิวเตอร์สำหรับการเลือกตั้ง

3.3 การรักษาความปลอดภัยในระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์

การรักษาความปลอดภัยในระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์ จะต้องครอบคลุมถึงเงื่อนไขดังต่อไปนี้

1. ระบบจะต้องสามารถตรวจสอบได้ว่าบัตรเลือกตั้งที่ได้รับจากหน่วยเลือกตั้งนั้น มาจากผู้ที่มีสิทธิ์เลือกตั้งตามกฎหมาย

2. ระบบจะต้องรักษาความลับของบัตรเลือกตั้ง โดยจะต้องป้องกันมิให้บุคคลที่มิได้รับอนุญาต สามารถอ่านข้อมูลภายในบัตรเลือกตั้งได้ และจะต้องป้องกันมิให้ผู้ใดมีส่วนร่วมในการออกเสียงเลือกตั้งร่วมกับผู้อื่น

3. ระบบจะต้องสามารถยืนยันได้ว่า จะต้องไม่มีบุคคลที่สาม หรือซอฟแวร์คอมพิวเตอร์ ที่จะสามารถเปลี่ยนแปลงข้อมูลในบัตรเลือกตั้งได้

4. ระบบจะต้องสามารถตรวจสอบการปลอมแปลง ความผิดพลาดและความเสียหายของบัตรเลือกตั้ง ที่ได้รับได้

5. ระบบจะต้องป้องกันมิให้ผู้มีสิทธิ์เลือกตั้ง สามารถทำการเลือกตั้งได้หลายครั้ง โดยที่ผู้มีสิทธิ์เลือกตั้งหนึ่งคน จะสามารถรับบัตรเลือกตั้งได้เพียงใบเดียว และจะต้องทำการเลือกตั้งได้เพียงหนึ่งครั้งเท่านั้น

6. ระบบจะต้องป้องกันมิให้ซอฟแวร์คอมพิวเตอร์ใด สามารถทำลายความเป็นส่วนตัวของผู้มีสิทธิ์เลือกตั้งได้

3.4 ขั้นตอนการรักษาความปลอดภัยในการรับส่งข้อมูล (Security Protocol)

ในระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์ จะประยุกต์ใช้การเข้ารหัสทั้งแบบสมมาตรหรือแบบทั่วไป (Symmetric Cryptography) และแบบไม่สมมาตรหรือแบบกุญแจสาธารณะ (Symmetric Cryptography) ร่วมกัน

การรวมกันของวิธีการเข้ารหัสสองวิธี เป็นการรวมความสะดวกของการเข้ารหัสแบบสาธารณะ กับความเร็วในการเข้ารหัสแบบทั่วไป เนื่องจากการเข้ารหัสแบบทั่วไปเร็วกว่าการเข้ารหัสแบบสาธารณะประมาณ 1000 เท่า แต่การเข้ารหัสแบบสาธารณะมีข้อดีในเรื่องวิธีแจกจ่ายรหัส ดังนั้นจึงนิยมใช้การเข้ารหัสข้อมูลซึ่งมีขนาดใหญ่ด้วยวิธีการเข้ารหัสแบบทั่วไป และใช้การเข้ารหัสแบบสาธารณะสำหรับการส่งกุญแจของการเข้ารหัสแบบทั่วไป โดยมีขั้นตอนดังต่อไปนี้

ส่วนที่ 1 การขอรับบัตรเลือกตั้ง

1. ระบบทำการตรวจสอบสิทธิ์การเลือกตั้งจากฐานข้อมูลผู้มีสิทธิ์เลือกตั้ง และตรวจสอบความถูกต้องของบัตรประจำตัวประชาชน

2. ผู้มีสิทธิ์เลือกตั้งจะต้องทำการยืนยันรหัส PIN ของบัตร

3. ระบบทำการอ่านหมายเลขประจำตัว (ID) จากบัตรประจำตัวประชาชนของผู้มีสิทธิ์เลือกตั้ง แล้วทำการเซ็นหมายเลขประจำตัวนั้น ด้วยกุญแจลับส่วนตัว (Private Key) ของเครื่องคอมพิวเตอร์ที่หน่วยเลือกตั้ง

4. จากนั้นระบบจะทำการสร้างกุญแจชั่วคราว (Session Key) แล้วทำการเข้ารหัสหมายเลขประจำตัว พร้อมกับลายเซ็นดิจิตอลที่ผู้มีสิทธิ์เลือกตั้งได้รับ ซึ่งเป็นการเข้ารหัสโดยใช้กุญแจแบบสมมาตร โดยใช้ Algorithm แบบ 3DES ความยาวกุญแจเป็น 128 บิต

5. ระบบทำการเข้ารหัสกุญแจชั่วคราว (Session Key) ด้วย กุญแจสาธารณะ (Public Key) ของหน่วยประมวลผลการเลือกตั้ง (Server) เพื่อสร้างความมั่นใจว่า เฉพาะหน่วยประมวลผลการเลือกตั้งเท่านั้นที่จะสามารถถอดรหัสกุญแจชั่วคราวได้

6. ทำการส่งข้อมูลที่เข้ารหัสแล้วทั้งหมด (หมายเลขประจำตัว + ลายเซ็นดิจิตอล กับกุญแจชั่วคราว) ไปให้หน่วยประมวลผลการเลือกตั้ง

7. หน่วยประมวลผลการเลือกตั้งรับข้อมูลจากหน่วยเลือกตั้ง แล้วใช้ กุญแจลับส่วนตัว (Private Key) ทำการถอดรหัสกุญแจชั่วคราว (Session Key)

8. แล้วใช้ กุญแจชั่วคราว (Session Key) ทำการถอดรหัสหมายเลขประจำตัวของผู้มีสิทธิ์เลือกตั้งกับลายเซ็นดิจิตอลของหน่วยเลือกตั้งออก

9. หน่วยประมวลผลการเลือกตั้งทำการตรวจสอบความถูกต้องของหมายเลขประจำตัวของผู้มีสิทธิ์เลือกตั้งจากลายเซ็นดิจิตอล โดยใช้ กุญแจสาธารณะ (Public Key) ของหน่วยเลือกตั้ง

10. หากลายเซ็นดิจิตอลมีความถูกต้อง ระบบจะทำการ Hash หมายเลขประจำตัวประชาชน โดยใช้ Algorithm แบบ MD5 แล้วทำการเก็บในฐานข้อมูล

11. ระบบจะทำการออกบัตรเลือกตั้ง (Ballot) จากฐานข้อมูลของบัตรเลือกตั้ง แล้วทำการจัดรูปแบบของบัตรเลือกตั้ง ดังต่อไปนี้

Ballot [Serial Number , SectionID , TotalCandidate , H[ID]]

Serial Number: หมายเลขลำดับบัตรเลือกตั้ง

SectionID: หมายเลขประจำเขตเลือกตั้ง

TotalCandidate: จำนวนผู้สมัครทั้งหมดในเขตเลือกตั้งนั้น

H[ID]: ค่า Hash ของหมายเลขประจำตัวของผู้รับบัตรเลือกตั้ง

12. หน่วยประมวลผลการเลือกตั้งทำการเซ็นบัตรเลือกตั้งด้วย กุญแจลับส่วนตัว (Private Key)

13. จากนั้นระบบทำการสร้างกุญแจชั่วคราว (Session Key) แล้วทำการเข้ารหัสบัตรเลือกตั้งและลายเซ็นดิจิตอลตามแบบข้อ 4

14. ระบบทำการเข้ารหัสกุญแจชั่วคราว (Session Key) ด้วย กุญแจสาธารณะ (Public Key) ของหน่วยเลือกตั้งตามแบบข้อ 5

15. หน่วยประมวลผลการเลือกตั้งทำการส่งข้อมูลที่เข้ารหัสแล้วทั้งหมด (บัตรเลือกตั้ง+ลายเซ็นดิจิตอล, กุญแจชั่วคราว) ไปให้หน่วยเลือกตั้งที่ได้ขอบัตรเลือกตั้ง

16. หน่วยเลือกตั้งรับข้อมูลจากหน่วยประมวลผล แล้วทำการถอดรหัสกุญแจชั่วคราว (Session Key) ด้วยกุญแจลับส่วนตัว (Private Key) ของหน่วยเลือกตั้ง

17. จากนั้นระบบจะทำการถอดรหัสบัตรเลือกตั้งและลายเซ็นดิจิตอลโดยใช้กุญแจชั่วคราว (Session Key)

18. หน่วยเลือกตั้งทำการตรวจสอบความถูกต้องของบัตรเลือกตั้ง จากลายเซ็นดิจิตอล โดยใช้ กุญแจสาธารณะ (Public Key) ของหน่วยประมวลผลการเลือกตั้ง

19. หากบัตรเลือกตั้งมีความถูกต้อง ระบบจะทำการบันทึกข้อมูลภายในบัตรเลือกตั้งลงในบัตรประชาชนของผู้มีสิทธิ์เลือกตั้ง

ส่วนที่ 2 การใช้สิทธิ์เลือกตั้ง

1. ระบบทำการตรวจสอบบัตรเลือกตั้งภายในบัตรประจำตัวประชาชน และผู้มีสิทธิ์เลือกตั้งจะต้องทำการยืนยันรหัส PIN ของบัตรอีกครั้ง

2. ระบบทำการอ่านบัตรเลือกตั้ง แล้วนำข้อมูลออกมาแสดง

3. ผู้มีสิทธิ์เลือกตั้งทำการเลือกผู้สมัคร ซึ่งจะได้รูปแบบของบัตรเลือกตั้ง (Ballot) ใหม่ ดังนี้

Ballot [Serial Number , SectionID , Candidate Number , H[ID]]

Serial Number: หมายเลขลำดับบัตรเลือกตั้ง

SectionID: หมายเลขประจำเขตเลือกตั้ง

Candidate Number: หมายเลขประจำตัวผู้สมัคร

H[ID]: ค่า Hash ของหมายเลขประจำตัวของผู้รับบัตรเลือกตั้ง

4. ระบบทำการเซ็นบัตรเลือกตั้งด้วยกุญแจลับส่วนตัว (Private Key)

5. ระบบทำการสร้างกุญแจชั่วคราว (Session Key) เพื่อเข้ารหัสบัตรเลือกตั้งและลายเซ็นดิจิตอล

6. ทำการเข้ารหัสกุญแจชั่วคราว (Session Key) ด้วยกุญแจสาธารณะ (Public Key) ของหน่วยประมวลผลการเลือกตั้ง

7. ระบบทำการส่งข้อมูลที่เข้ารหัสทั้งหมด (บัตรเลือกตั้ง+ลายเซ็นดิจิตอล, กุญแจชั่วคราว) ไปให้หน่วยประมวลผลการเลือกตั้ง

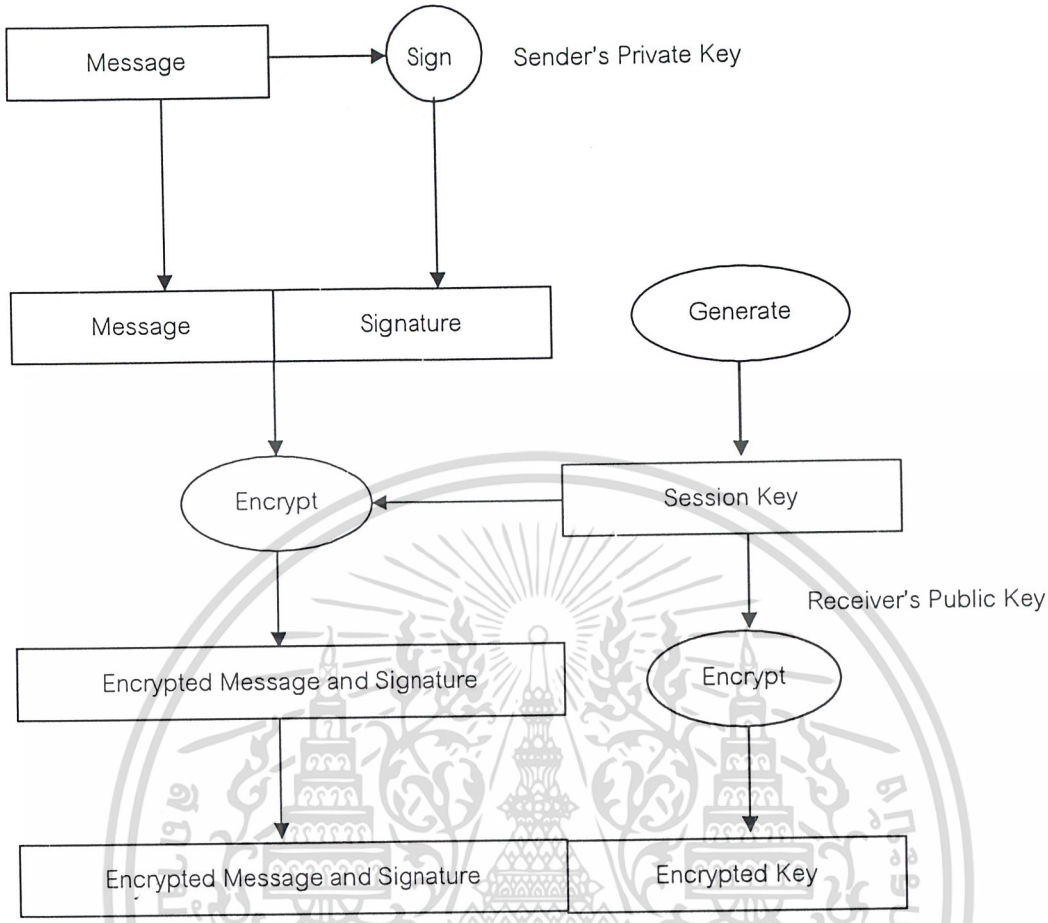
8. ระบบทำการลบบัตรเลือกตั้ง ที่บันทึกอยู่ในบัตรประจำตัวประชาชน เพื่อป้องกันมิให้ผู้มีสิทธิ์เลือกตั้งทำการเลือกตั้งซ้ำได้อีก

9. หน่วยประมวลผลการเลือกตั้งรับบัตรเลือกตั้งจากหน่วยเลือกตั้ง แล้วทำการถอดรหัสกุญแจชั่วคราว (Session Key) ด้วยกุญแจลับส่วนตัว (Private Key)

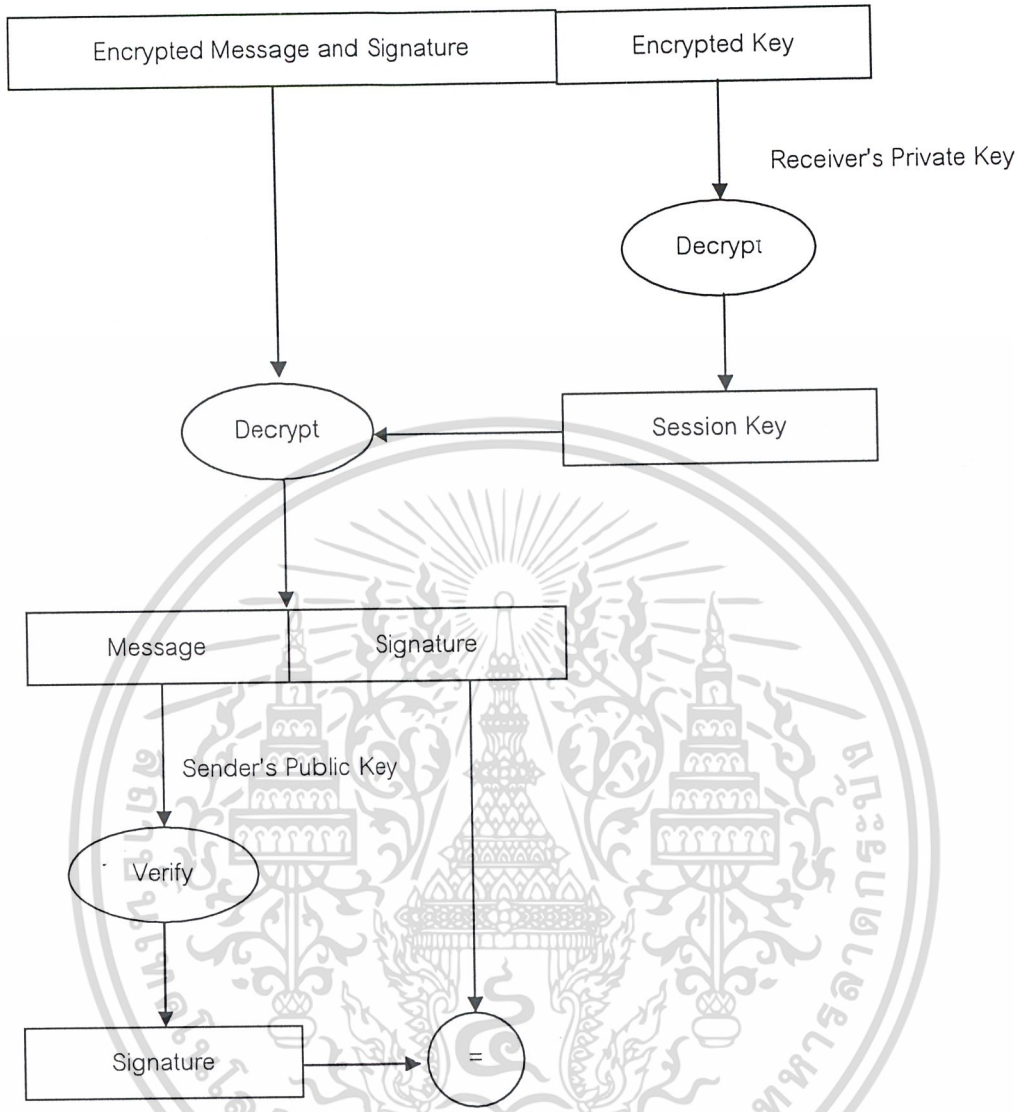
10. จากนั้นใช้กุญแจชั่วคราว (Session Key) ถอดรหัสบัตรเลือกตั้งและลายเซ็นดิจิตอล

11. ทำการตรวจสอบความถูกต้องของบัตรเลือกตั้งที่ส่งกลับมา ด้วยลายเซ็นดิจิตอล โดยใช้กุญแจสาธารณะ (Public Key) ของเครื่องคอมพิวเตอร์ที่ทำการเลือกตั้ง

12. ถ้าบัตรเลือกตั้งมีความถูกต้อง ระบบจะทำการเก็บบัตรเลือกตั้งนั้นไว้ในฐานข้อมูล แล้วเปลี่ยนสถานะ การเลือกตั้งของผู้มีสิทธิ์เลือกตั้ง โดยเปรียบเทียบกับ H(ID) ที่อยู่ภายในบัตรเลือกตั้ง และทำการลบ H(ID) ออกจากบัตรเลือกตั้งและฐานข้อมูลทันที



รูปที่ 3.6 รูปแบบการเข้ารหัสข้อมูลที่ใช้ในระบบเลือกตั้ง



รูปที่ 3.7 รูปแบบการเข้าถอดรหัสข้อมูลที่ใช้ในระบบเลือกตั้ง

3.5 System Specification

1. Database Server

- ระบบปฏิบัติการ Windows 2000 Server
- ระบบจัดการฐานข้อมูลเชิงสัมพันธ์ Microsoft SQL 2000 Server
- ระบบจัดการโครงสร้างพื้นฐานกุญแจสาธารณะ

2. Certification Authority Server

- ระบบปฏิบัติการ Windows 2000 Server
- ระบบบริการออกใบรับรองดิจิตอลประเภท Stand Alone Certification Authority
- Internet Information Service 5.0

3. ระบบคอมพิวเตอร์สำหรับงานทะเบียน และการเลือกตั้ง

- ระบบปฏิบัติการ Windows 98, 2000
- เครื่องเขียน-อ่านบัตร สมาร์ตการ์ด

บทที่ 4

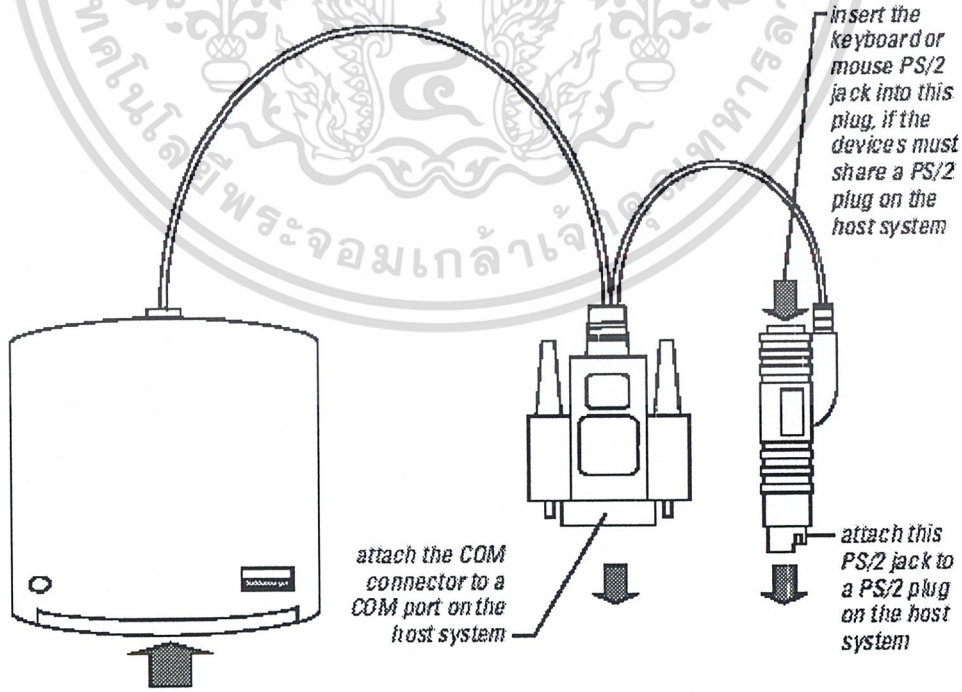
ผลการทดลอง

จากการออกแบบระบบในบทที่ผ่านมา ทำให้สามารถแยกการทำงานของระบบออกเป็น 2 ส่วน คือ 1. ระบบงานทะเบียนและการออกบัตรประจำตัวประชาชน และ 2. ระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์ ซึ่งทั้ง 2 ระบบ จะทำงานสัมพันธ์ซึ่งกันและกัน โดยมีรายละเอียดดังต่อไปนี้

4.1 ระบบงานทะเบียนและการออกบัตรประจำตัวประชาชน

การติดตั้งเครื่องอ่านบัตรสมาร์ตการ์ด (Schlumberger Reflex 72 Smart Card Reader)

1. ทำการปิดเครื่องคอมพิวเตอร์
2. ติดตั้งเครื่องอ่านบัตรสมาร์ตการ์ด เข้ากับ COM พอร์ต ซึ่งเป็นช่องทางการสื่อสารระหว่างเครื่องอ่านบัตรกับคอมพิวเตอร์
3. ทำการติดตั้งแหล่งจ่ายไฟฟ้าให้แก่เครื่องอ่านบัตรสมาร์ตการ์ด โดยต่อเข้ากับ พอร์ตชนิด PS/2 ดังรูป

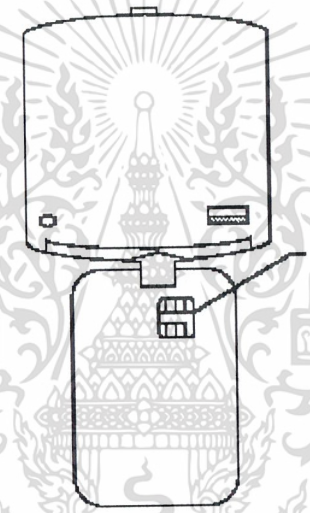


รูปที่ 4.1 การติดตั้งเครื่องอ่านสมาร์ตการ์ด

4. เปิดเครื่องคอมพิวเตอร์ ระบบปฏิบัติการ (Windows 98, ME, NT, 2000, XP) จะทำการตรวจสอบและทำการติดตั้ง Driver ของเครื่องอ่านสมาร์ตการ์ด ให้โดยอัตโนมัติ

การสอดบัตรสมาร์ตการ์ดเข้าสู่เครื่องอ่านบัตร

1. การสอดบัตรสมาร์ตการ์ดเข้าสู่เครื่องอ่านบัตรอย่างถูกต้อง จะต้องหงายด้านที่มีหน้าสัมผัสขึ้น และหันด้านที่อยู่ใกล้กับหน้าสัมผัสเข้าสู่เครื่องอ่านบัตร ดังรูป



รูปที่ 4.2 การสอดบัตรสมาร์ตการ์ดเข้าสู่เครื่องอ่านบัตรอย่างถูกต้อง

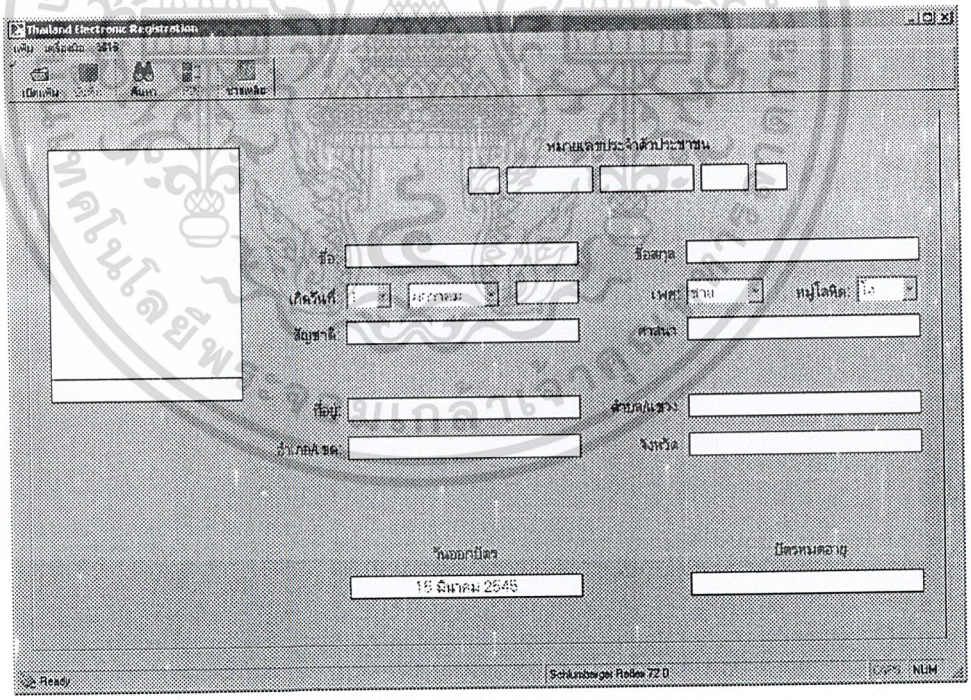
2. ค่อย ๆ ดันบัตรเข้าไปในเครื่องอ่านบัตรจนสุด จนหลอดไฟ LED ที่อยู่บนเครื่องอ่านบัตรสว่าง

การทำงานของระบบงานทะเบียนและการออกบัตรประจำตัวประชาชน

1. เมื่อระบบเริ่มทำงาน ระบบจะทำการตรวจสอบการว่ามีเครื่องอ่านบัตรสมาร์ตการ์ดติดตั้งอยู่หรือไม่ และทดสอบการติดต่อไปยังศูนย์ทะเบียนกลาง ซึ่งถ้ามีอย่างหนึ่งอย่างใดไม่พร้อมทำงาน โปรแกรมก็จะแสดงข้อความผิดพลาด

รูปที่ 4.3 ระบบทำการตรวจสอบเครื่องอ่านบัตรสมาร์ตการ์ด

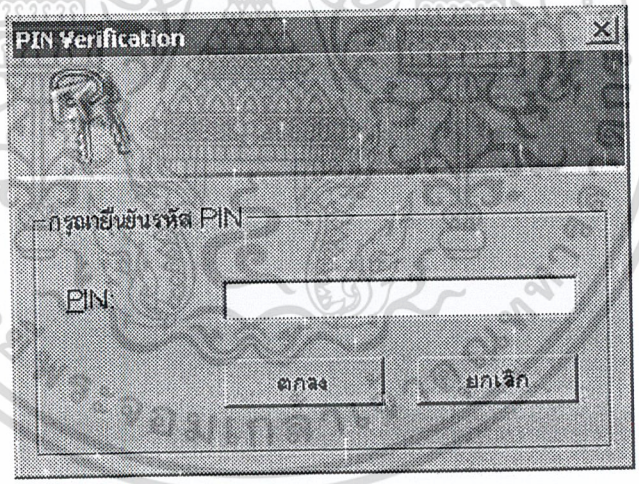
2. เมื่อระบบพร้อมสำหรับการทำงาน ก็จะแสดงหน้าจอหลักของ โปรแกรมลงทะเบียน



รูปที่ 4.4 หน้าจอหลักของโปรแกรมลงทะเบียน

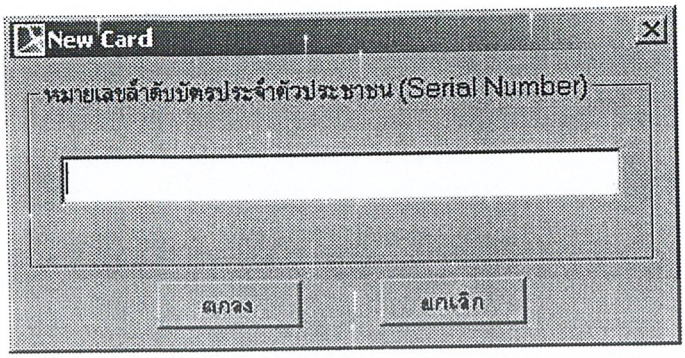
3. การทำบัตรประจำตัวประชาชนเป็นครั้งแรก หรือการทำบัตรใหม่เนื่องจากบัตรเก่าหมดอายุ เจ้าหน้าที่จะต้องทำการสอดบัตรใหม่เข้าไปในเครื่องอ่านบัตร จากนั้นโปรแกรมก็จะทำการติดต่อกับบัตรให้โดยอัตโนมัติ และทำการตรวจสอบคุณสมบัติต่าง ๆ ดังนี้
    1. ตรวจสอบการทำงานของเครื่องอ่านบัตร
    2. ตรวจสอบค่า Answer to Reset ของบัตร
    3. ตรวจสอบโปรแกรมภายในบัตร
    4. ตรวจสอบวันหมดอายุของบัตร

4. เมื่อคุณสมบัติของบัตรทุกอย่างถูกต้อง เจ้าหน้าที่ก็จะต้องทำการยืนยันรหัส PIN เพื่ออนุญาตให้มีการเขียนข้อมูลลงในบัตรได้ ซึ่งการยืนยันรหัส PIN จะสามารถทำได้เพียง 10 ครั้งเท่านั้น ถ้าหากไม่สามารถยืนยัน PIN ได้ถูกต้องภายใน 10 ครั้ง บัตรก็จะถูกล็อคและจะใช้งานไม่ได้จนกว่าจะมีการปลดล็อค PIN



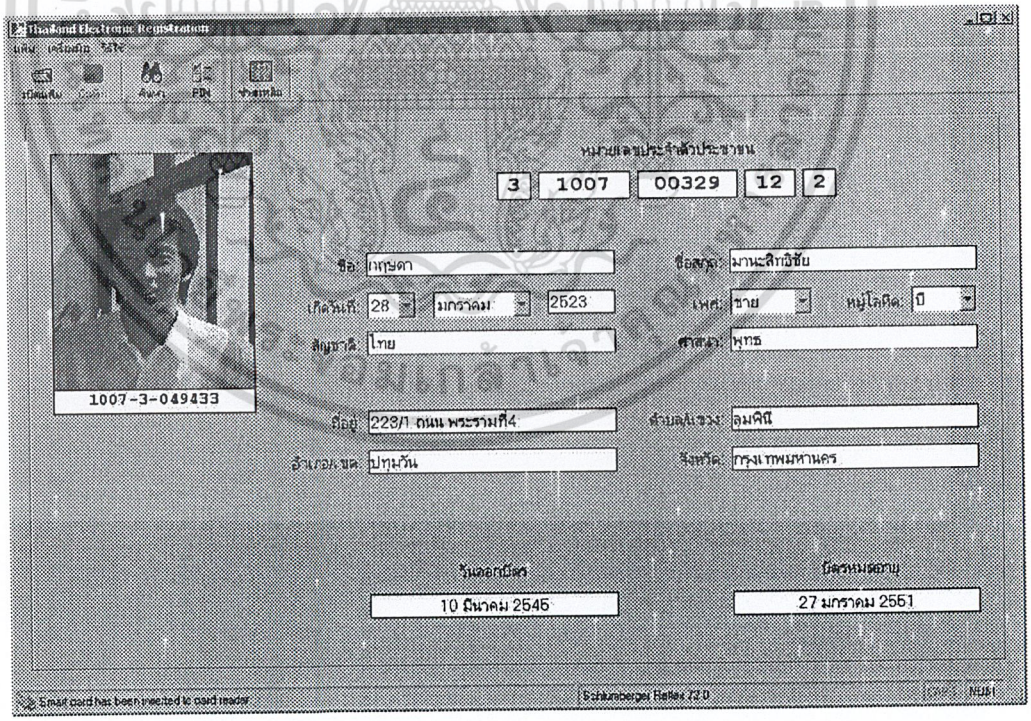
รูปที่ 4.5 หน้าจอแสดงการยืนยันรหัส PIN

5. จากนั้นเจ้าหน้าที่ก็จะต้องทำการใส่หมายเลขลำดับของบัตรประจำตัวประชาชน ดังรูป



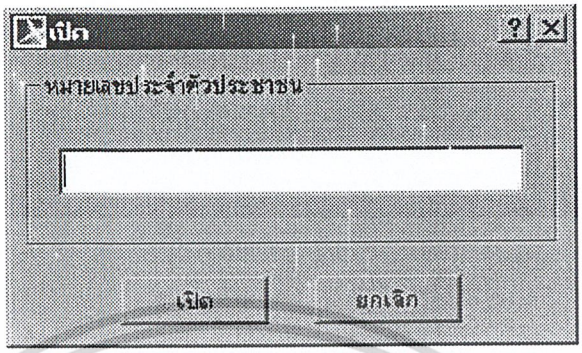
รูปที่ 4.6 หน้าจอแสดงการใส่หมายเลขลำดับบัตรประจำตัวประชาชน

6. เมื่อทำการใส่หมายเลขลำดับบัตรประจำตัวประชาชนเรียบร้อยแล้ว เจ้าหน้าที่ก็จะสามารถกรอกข้อมูลของเจ้าของบัตร, ถ่ายรูปเจ้าของบัตร และบันทึกข้อมูลลงสู่บัตรประจำตัวประชาชน และ ฐานข้อมูลทะเบียน เป็นอันเสร็จสิ้นกระบวนการออกบัตรประจำตัวประชาชน ดังรูป

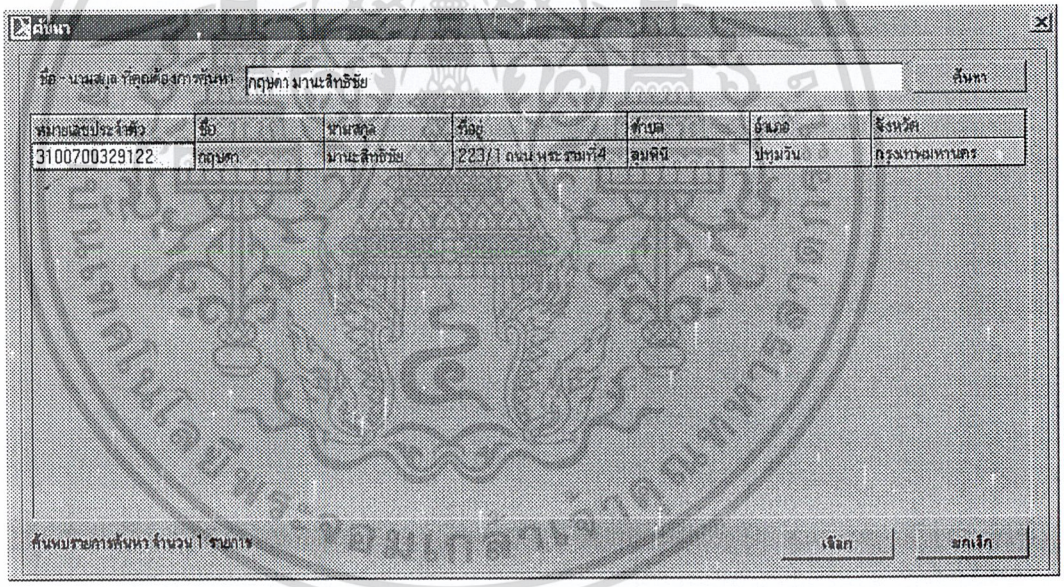


รูปที่ 4.7 หน้าจอแสดงข้อมูลของเจ้าของบัตรประจำตัวประชาชน

7. ถ้าหากผู้ที่มาทำบัตรประจำตัวประชาชนใหม่ เนื่องจากบัตรเก่าสูญหาย เจ้าหน้าที่ก็จะสามารถเปิดข้อมูล หรือทำการค้นหารายชื่อของผู้นั้นได้

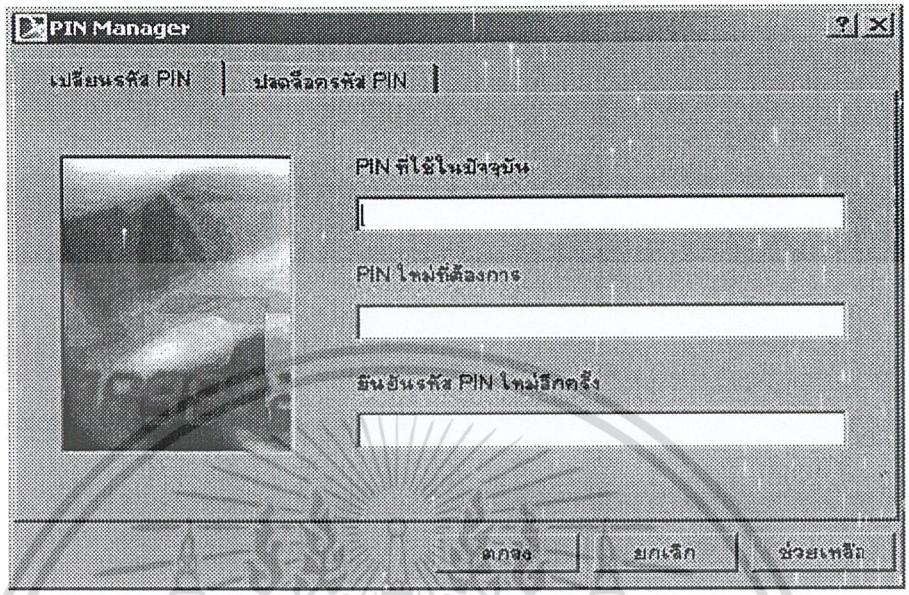


รูปที่ 4.8 หน้าจอแสดงการเปิดข้อมูล



รูปที่ 4.9 หน้าจอแสดงการค้นหาข้อมูลของประชาชน

8. หากเจ้าของบัตรต้องการเปลี่ยนรหัส PIN หรือทำการ Unblock PIN ก็สามารถทำได้ทันที



รูปที่ 4.10 หน้าจอแสดงการเปลี่ยนรหัส PIN และ Unblock PIN

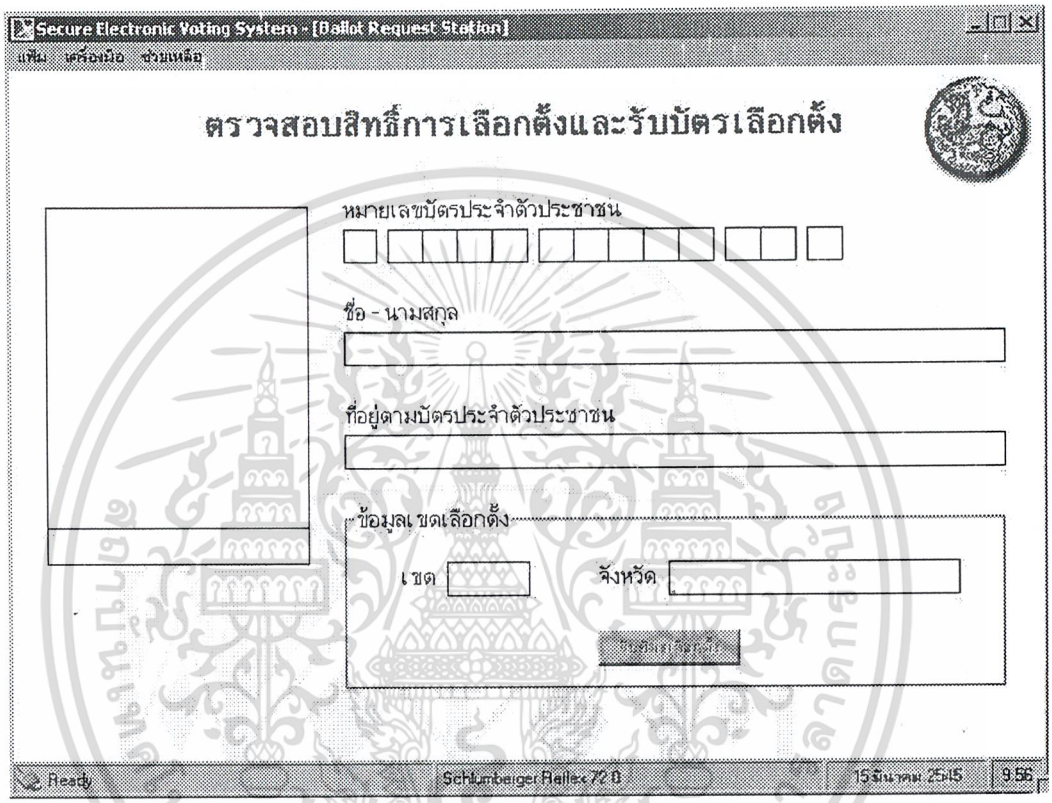
4.2 ระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์

4.2.1 ผลที่คาดว่าจะได้รับ

- ลดการใช้เอกสาร แบบพิมพ์ และสถานที่จัดเก็บ
- เพิ่มความสะดวกให้แก่ผู้ใช้สิทธิ์เลือกตั้ง ทำให้มีผู้ไปใช้สิทธิ์เลือกตั้งเพิ่มมากขึ้น
- ลดจำนวนบัตรเลือกตั้งเสีย
- ลดจำนวนการทุจริตการเลือกตั้ง
- กระตุ้นให้ประชาชนเห็นความสำคัญของระบบรักษาความปลอดภัยคอมพิวเตอร์

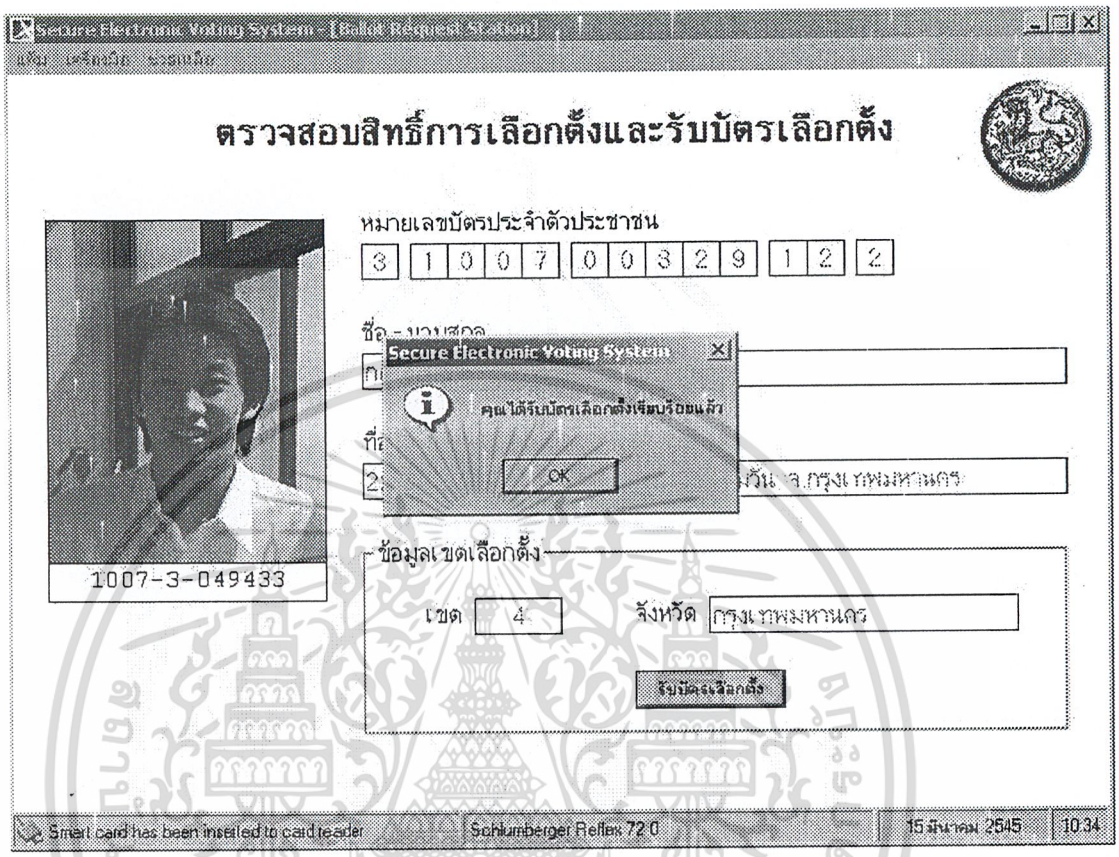
4.2.2 การทำงานของโปรแกรม

1. ผู้ที่มีสิทธิ์เลือกตั้งทำการตรวจสอบสิทธิ์การเลือกตั้งและรับบัตรเลือกตั้งที่หน่วยเลือกตั้ง โดยที่บัตรเลือกตั้งที่ได้รับมานั้น จะถูกเข้ารหัส ด้วยเทคโนโลยี PKI



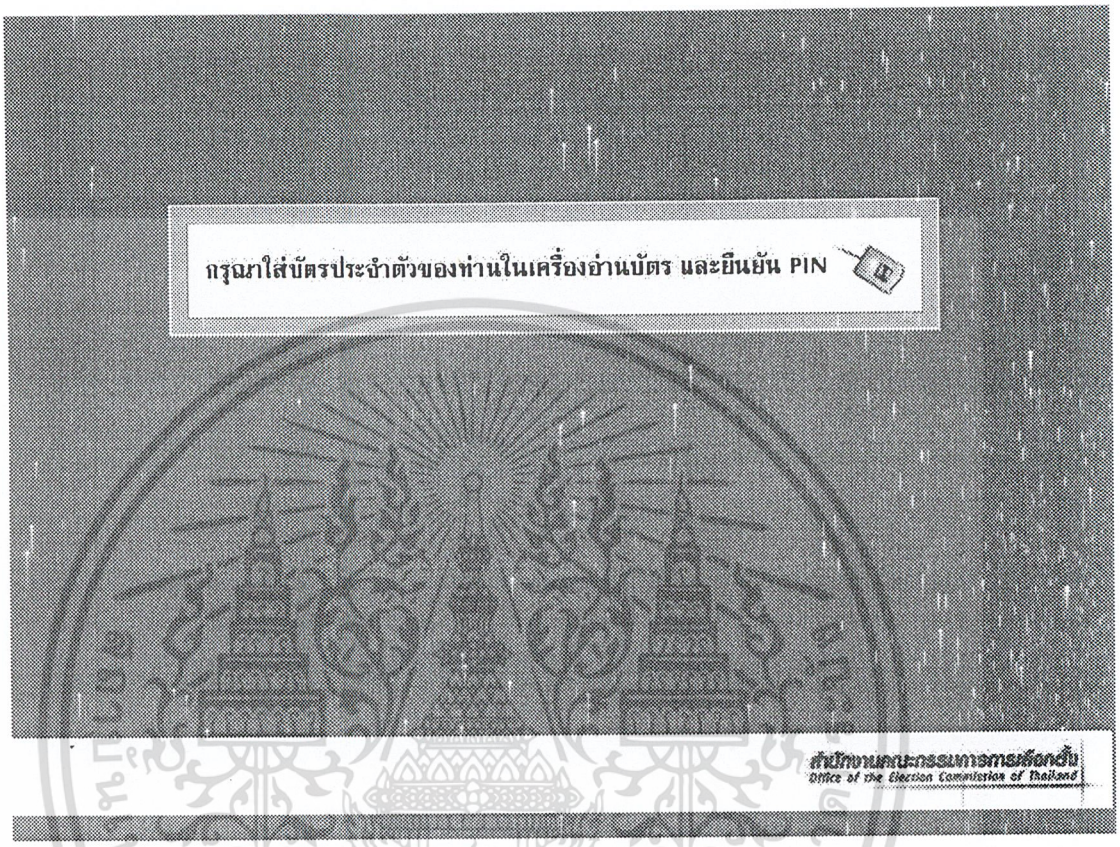
รูปที่ 4.11 หน้าจอแสดงการตรวจสอบสิทธิ์การเลือกตั้งและรับบัตรเลือกตั้ง

2. ระบบทำการบันทึกบัตรเลือกตั้งลงในบัตรประจำตัวของผู้มีสิทธิ์เลือกตั้ง



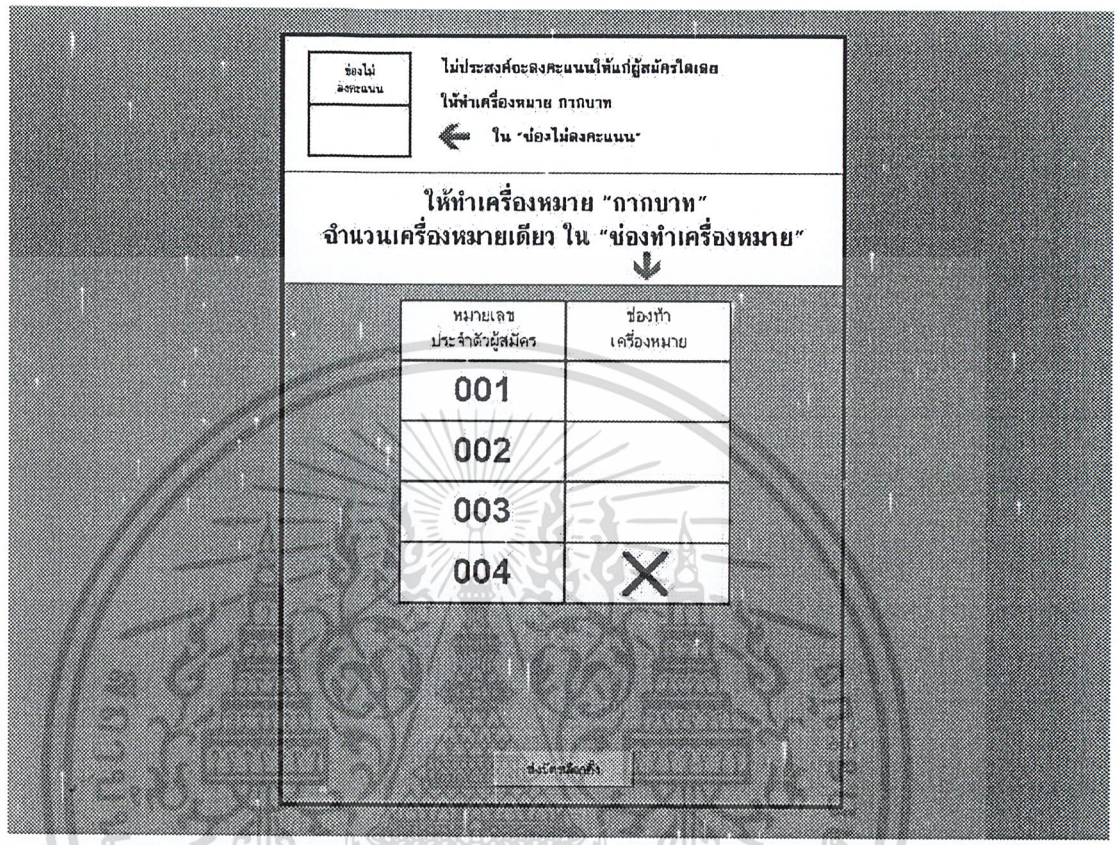
รูปที่ 4.12 หน้าจอแสดงการรับบัตรเลือกตั้ง

3. ผู้มีสิทธิ์เลือกตั้ง ทำการเลือกผู้สมัคร โดยระบบจะทำการอ่านข้อมูลบัตรเลือกตั้งจากบัตรประจำตัวของผู้มีสิทธิ์เลือกตั้ง



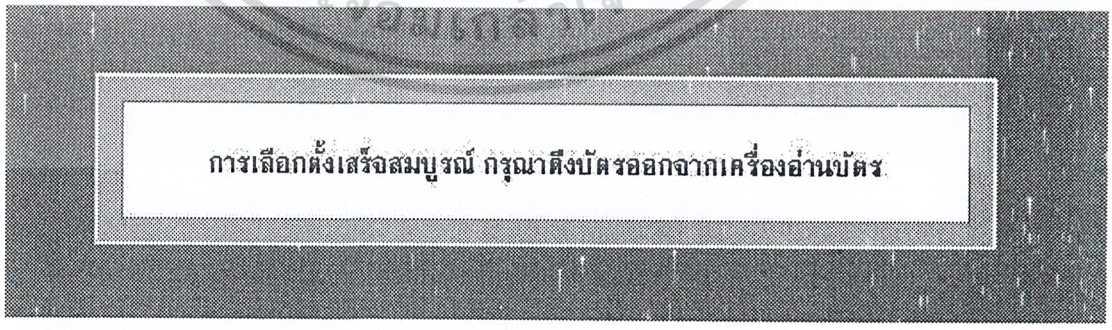
รูปที่ 4.13 หน้าจอแสดงต้อนรับการเลือกตั้ง

4. ระบบทำการแสดงบัตรเลือกตั้ง เพื่อให้ผู้มีสิทธิ์เลือกตั้งทำการเลือกผู้สมัคร



รูปที่ 4.14 หน้าจอแสดงการออกเสียงเลือกตั้ง

5. ระบบทำการยืนยันการเลือกตั้งเสร็จสมบูรณ์



รูปที่ 4.15 หน้าจอแสดงการยืนยันการเลือกตั้งเสร็จสมบูรณ์

บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

ปริญญานิพนธ์ฉบับนี้นำเสนอ ระบบงานทะเบียนและการออกบัตร และระบบการเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์ ระบบโดยรวมทำงานได้เป็นอย่างดีระดับหนึ่ง สามารถนำไปใช้เป็นระบบต้นแบบการออกบัตรประชาชนโดยใช้บัตรสมาร์ตการ์ดที่จะพัฒนาขึ้นในอนาคต ในโครงการ E – Government ได้ ส่วนระบบเลือกตั้งผ่านเครือข่ายคอมพิวเตอร์นั้น การ Authentication เจ้าของบัตรยังใช้แค่การยืนยันรหัส PIN เท่านั้น ซึ่งยังไม่มีความปลอดภัยเพียงพอที่จะนำไปใช้จริง ซึ่งหากมีการนำระบบนี้ไปพัฒนาต่อ โดยนำเอาเทคโนโลยี Biometric เช่น ระบบตรวจสอบลายนิ้วมือ, ฝ่ามือ, รูม่านตา เข้ามาประยุกต์แล้ว ก็จะทำให้ระบบมีความปลอดภัยมากยิ่งขึ้น

ปัญหาที่พบจากการพัฒนาระบบเกิดจากการที่มีอุปกรณ์ในการทดสอบระบบมีจำนวนน้อยเกินไป เพราะอุปกรณ์มีราคาค่อนข้างสูง หาซื้อยาก

ภาคผนวก

การออกแบบระบบ

รูปแบบการแสดงการออกแบบระบบ

- Client Interview

  แสดงขั้นตอนการทำงานในมุมมองของผู้ใช้

- High Level Use Case

  แสดงกิจกรรมทั้งหมดที่ของระบบประกอบไปด้วยผู้กระทำดังนี้

  Officer = เจ้าหน้าที่นายทะเบียนของระบบการทำบัตรและการเลือกตั้ง

  Citizen = ประชาชนผู้มีสิทธิทำบัตร

  Voter = ผู้เลือกตั้งของระบบ

  Crypto Service = โปรแกรมบริการการเข้ารหัสระหว่างเครื่องคอมพิวเตอร์ในเครือข่าย

  Voting Server = เครื่องให้บริการระบบการเลือกตั้ง

- Use Case

  แสดงเฉพาะกิจกรรมที่สำคัญจาก High Level Use Case

- Activity Diagram

  แสดงขั้นตอนการทำงานของกิจกรรมที่สำคัญจาก Use Case โดยละเอียด

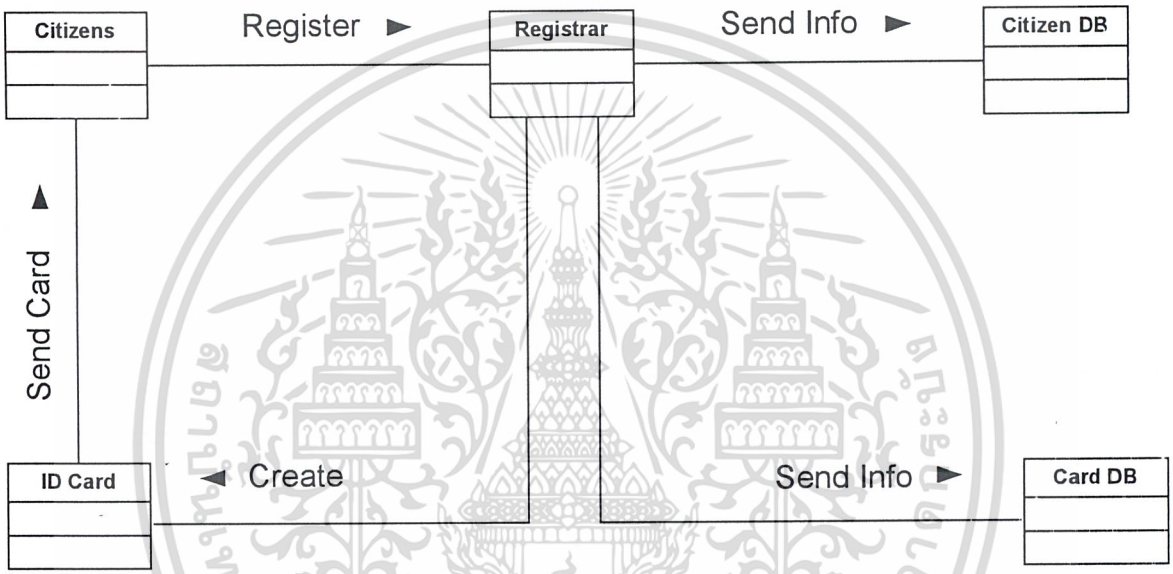
- NIAM

  แสดงความสัมพันธ์ของฐานข้อมูลในรูปความสัมพันธ์รูปแบบ NIAM และ ตาราง

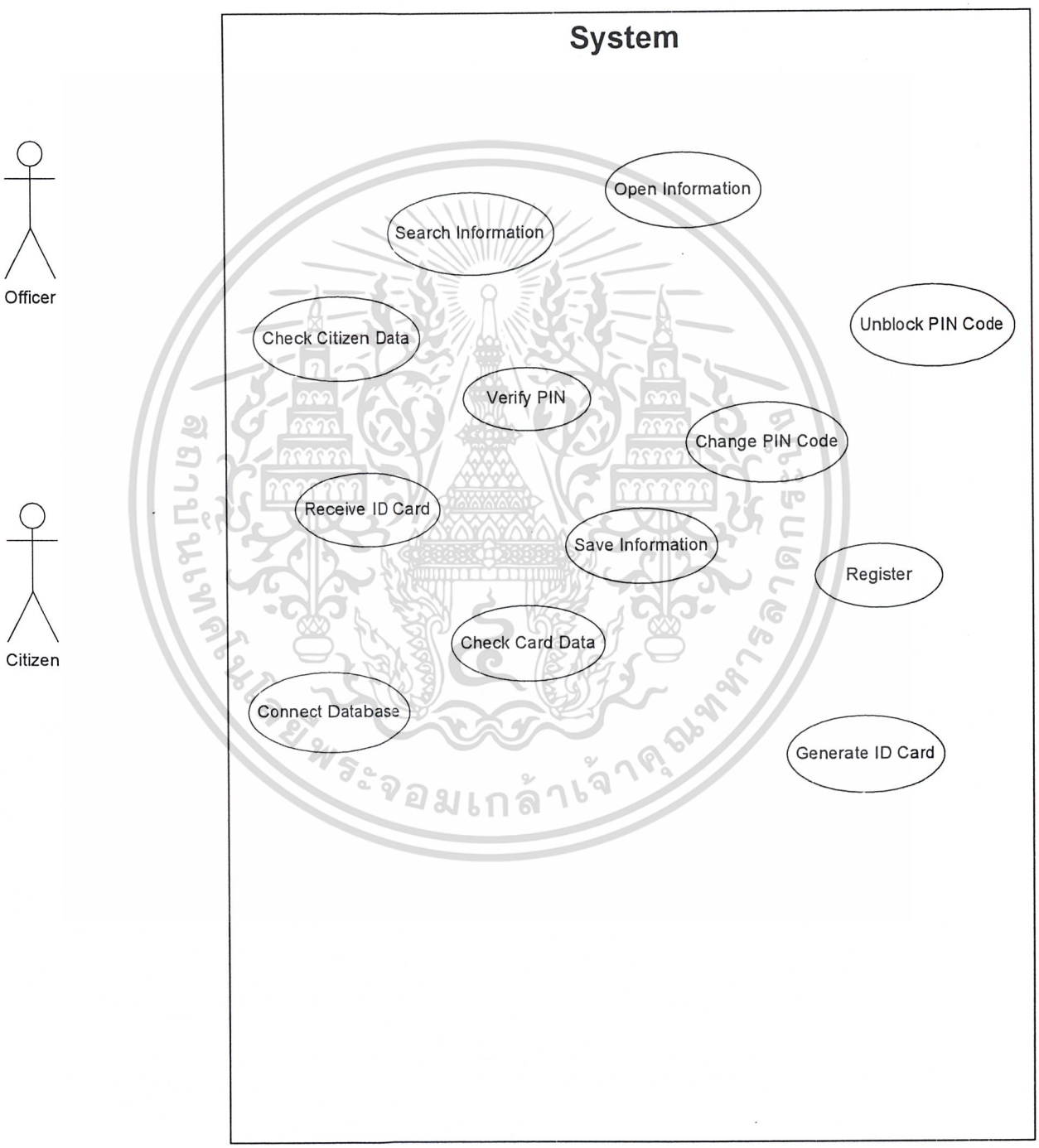
โดยในภาคผนวกนี้จะแสดงรูปแบบการแสดงการออกแบบระบบเป็น 2 ขั้นตอนคือ Register Phase (การออกบัตรประจำตัวประชาชน) และ Voting Phase (การเลือกตั้ง) ตามลำดับ

Register Phase

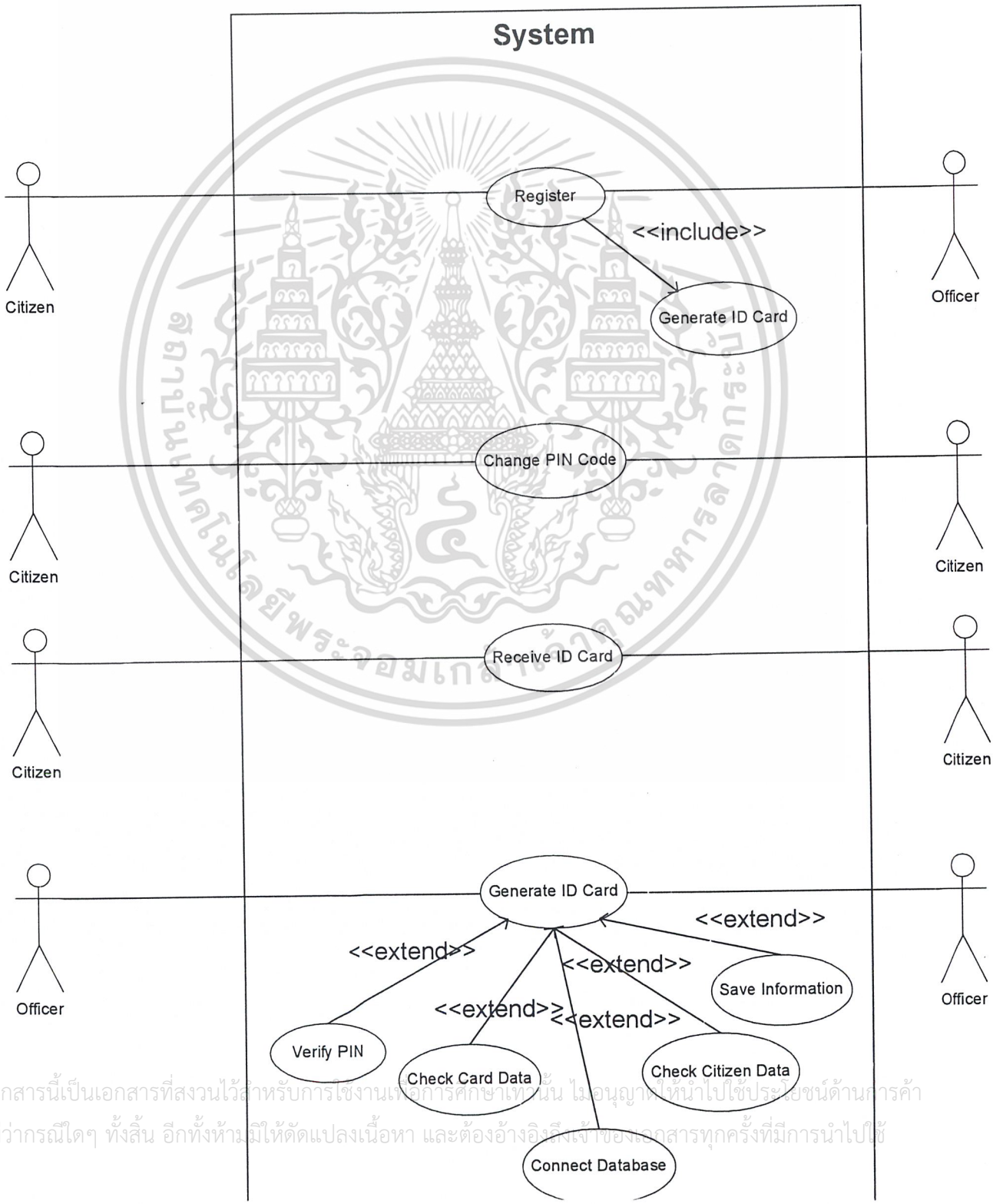
Client Interview



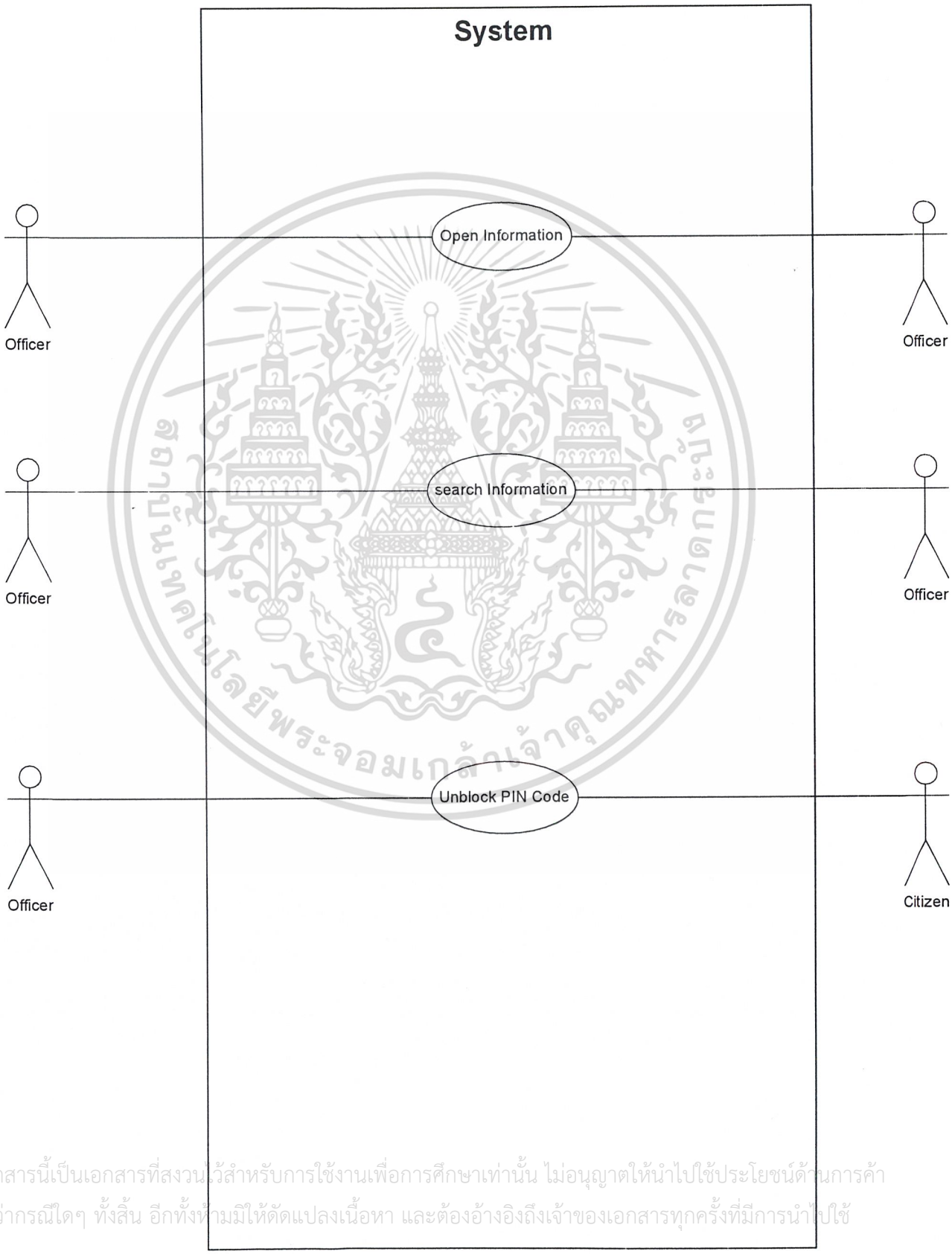
High Level Use Case



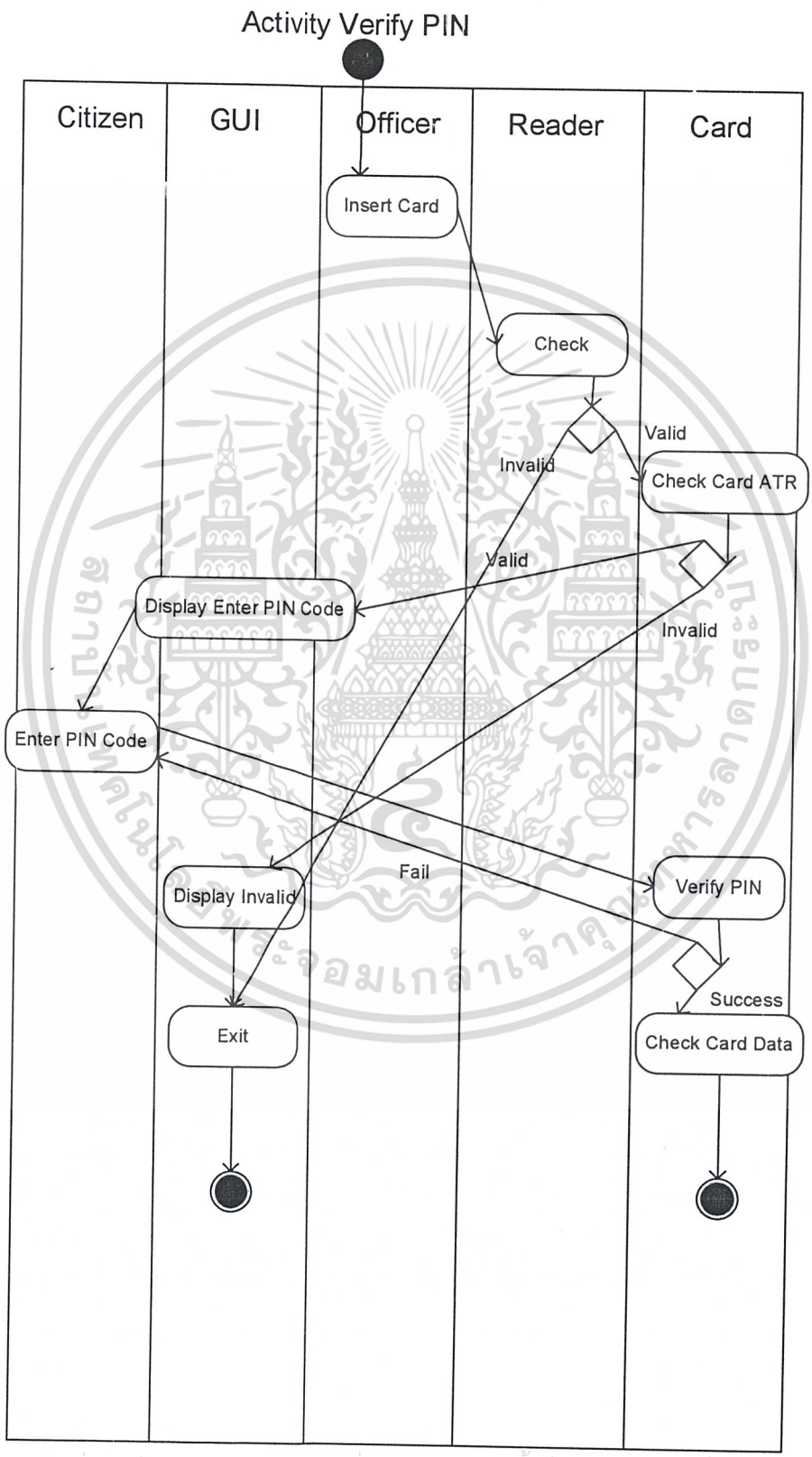
Use Case



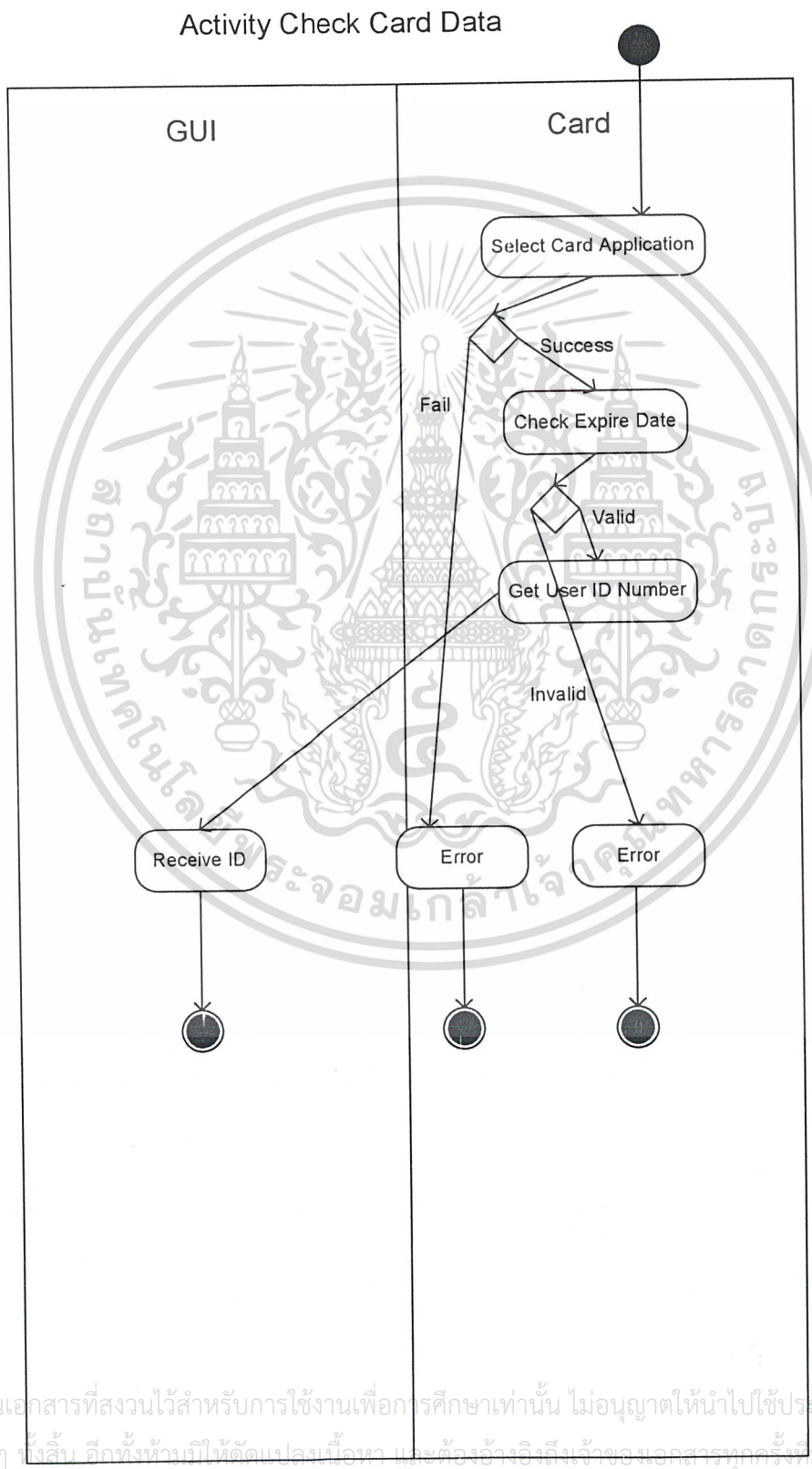
Use Case (Continue)



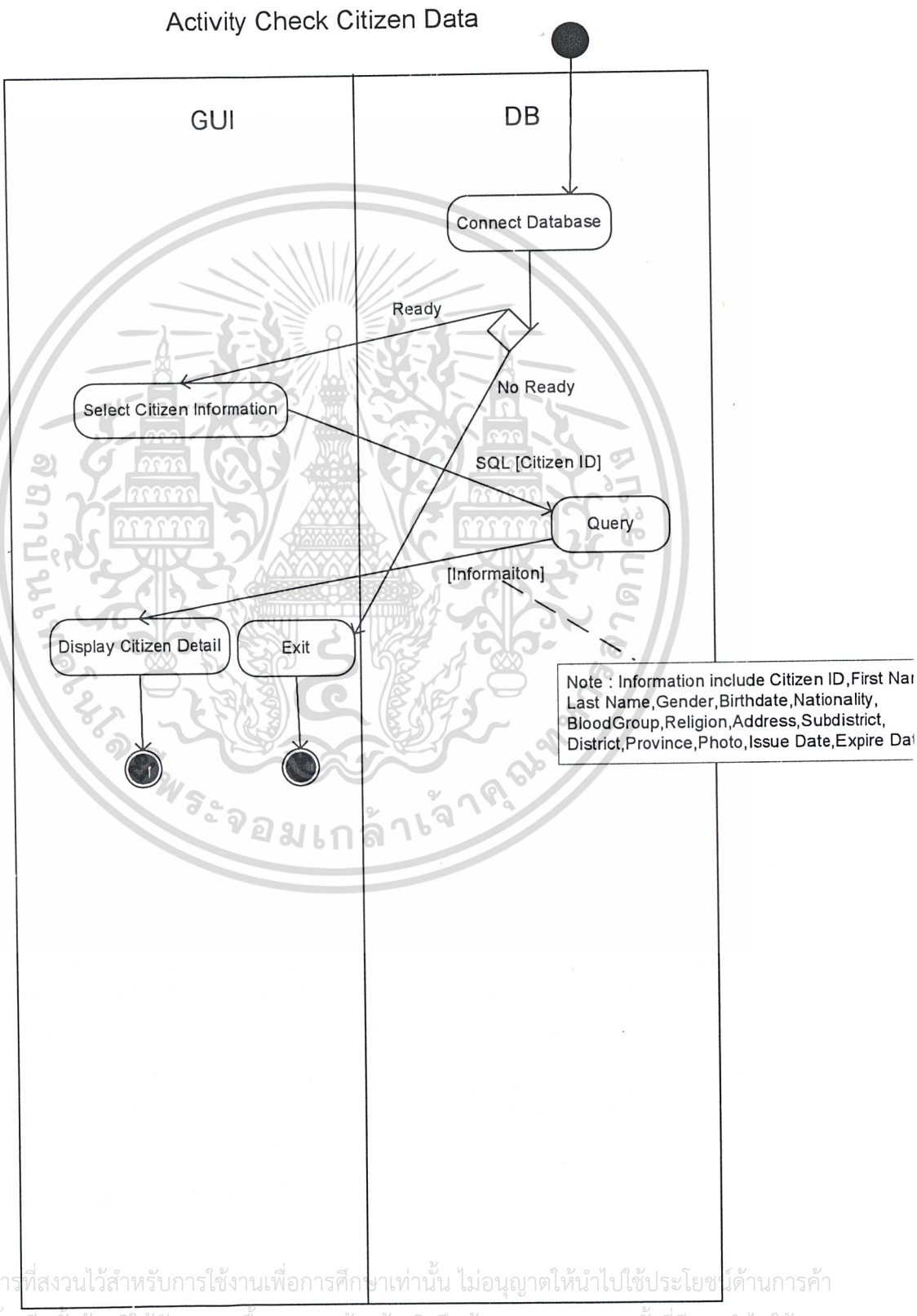
Activity Diagram



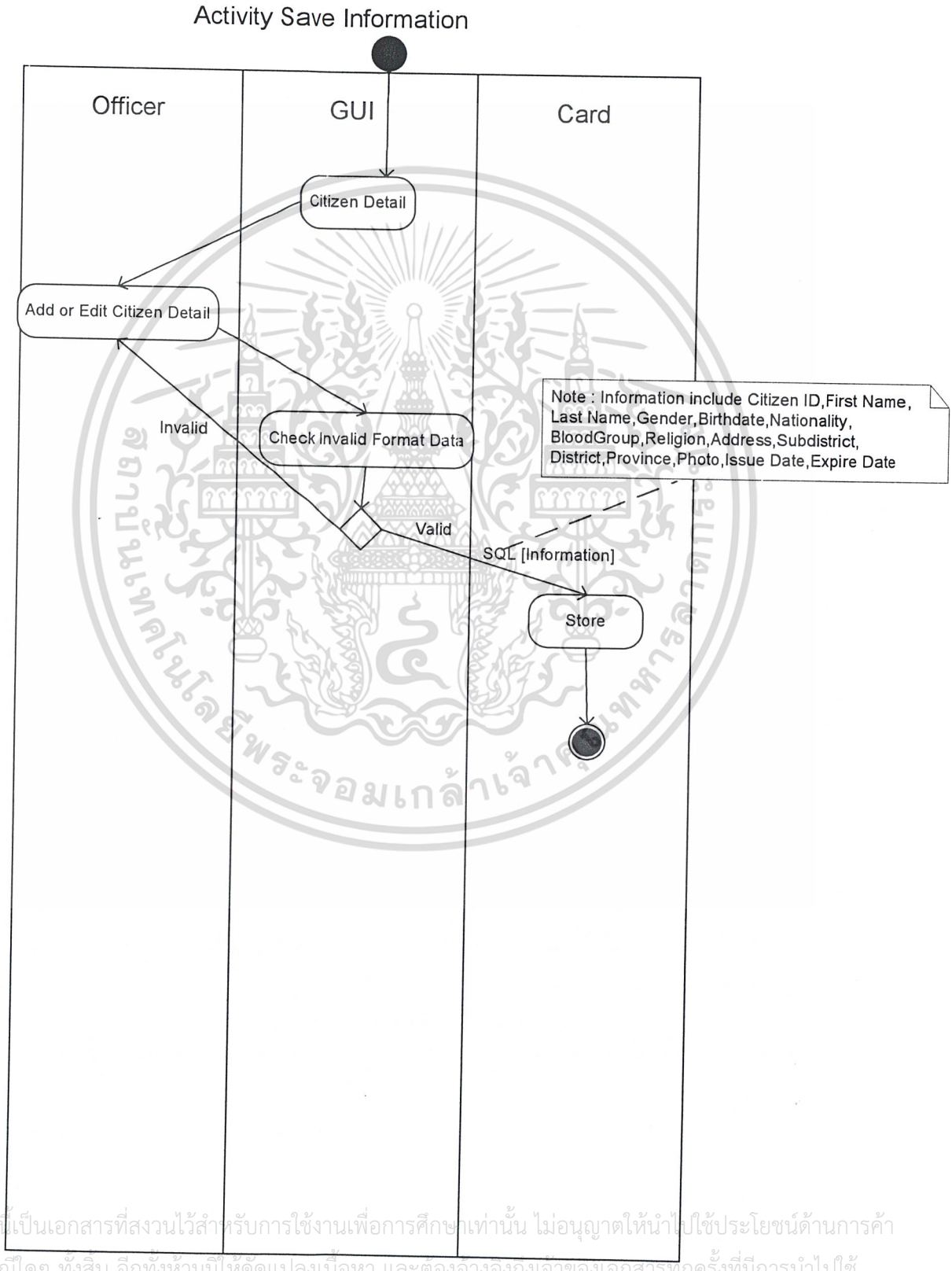
Activity Diagram (Continue)



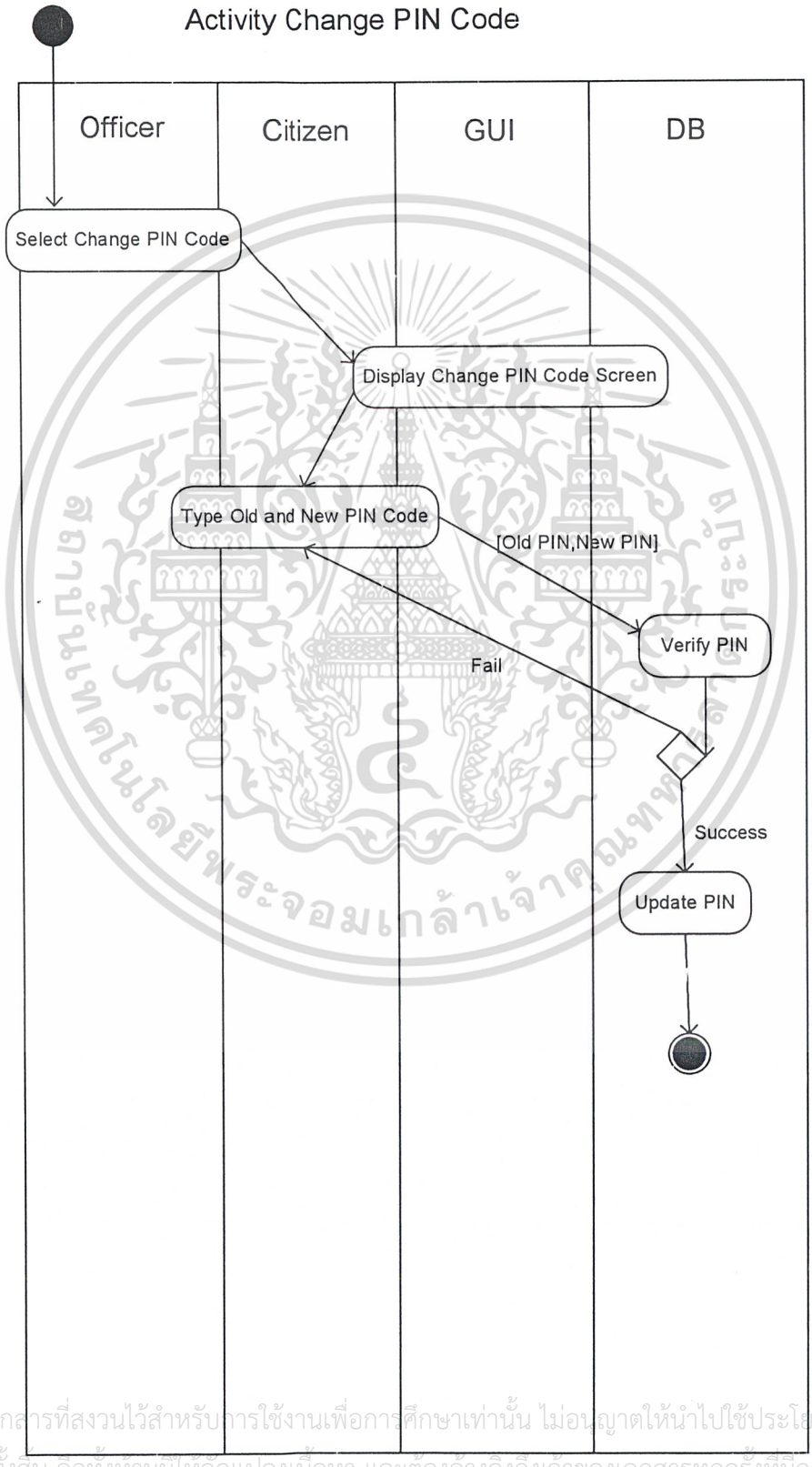
Activity Diagram (Continue)



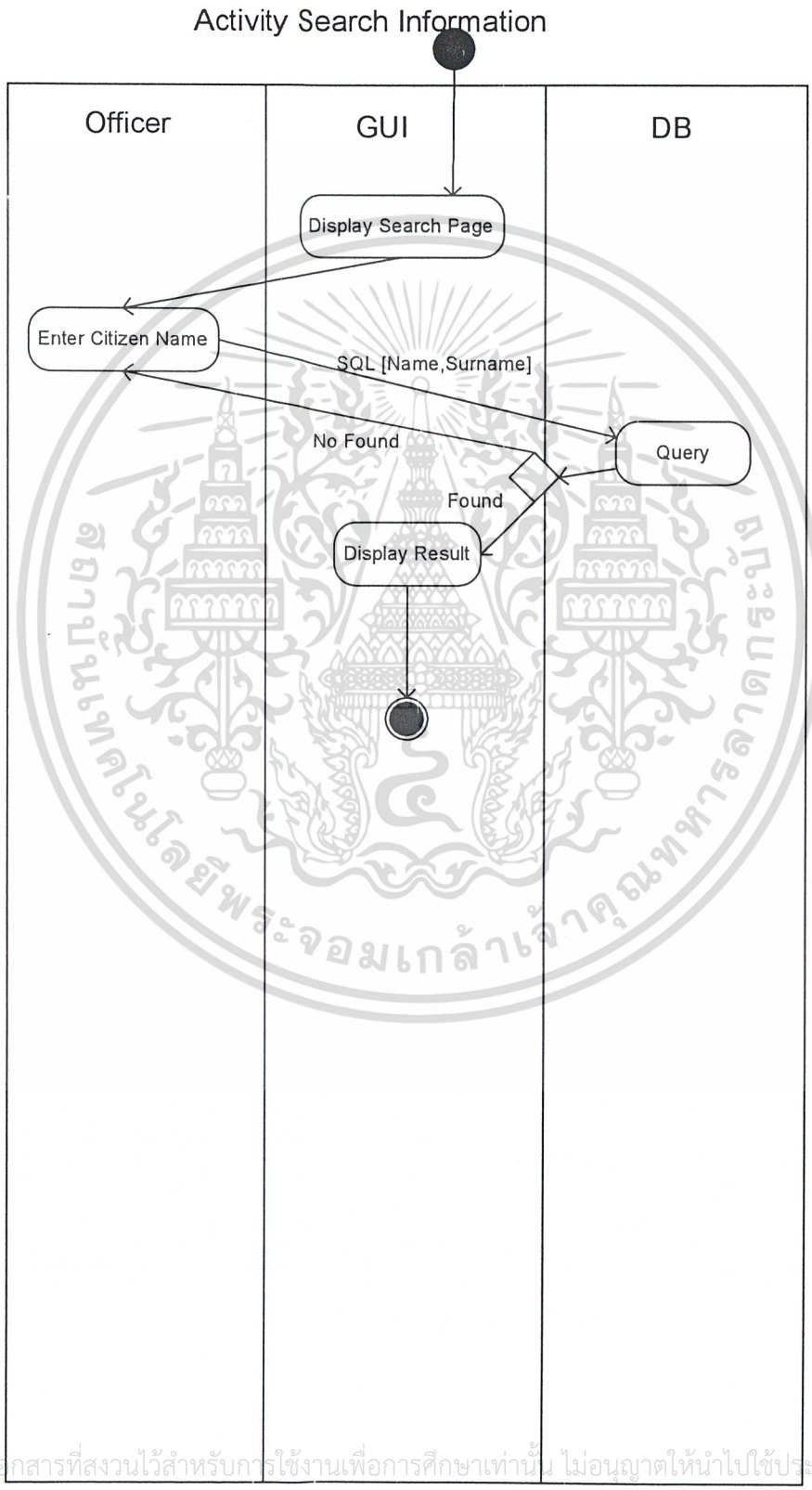
Activity Diagram (Continue)



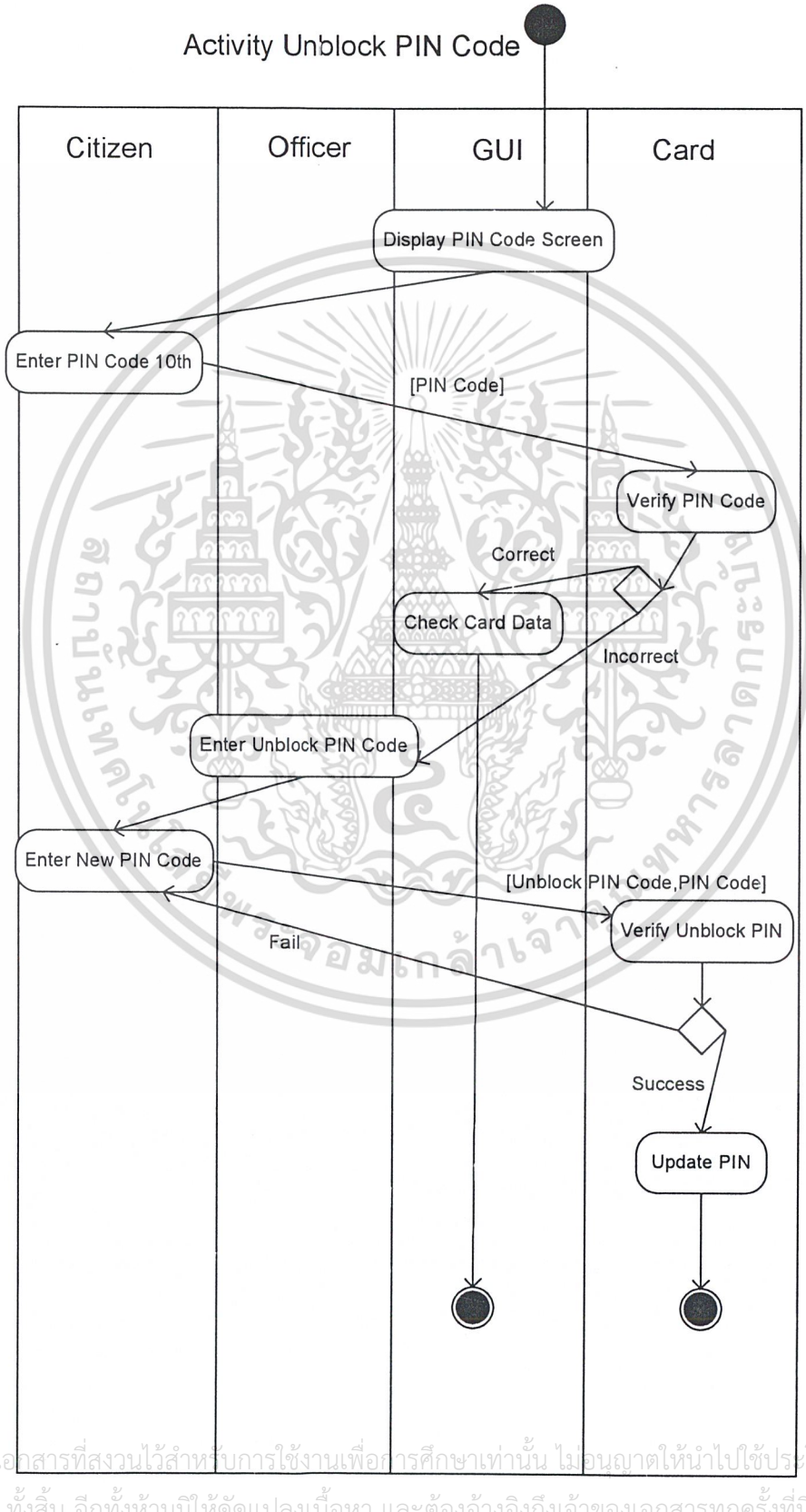
Activity Diagram (Continue)



Activity Diagram (Continue)

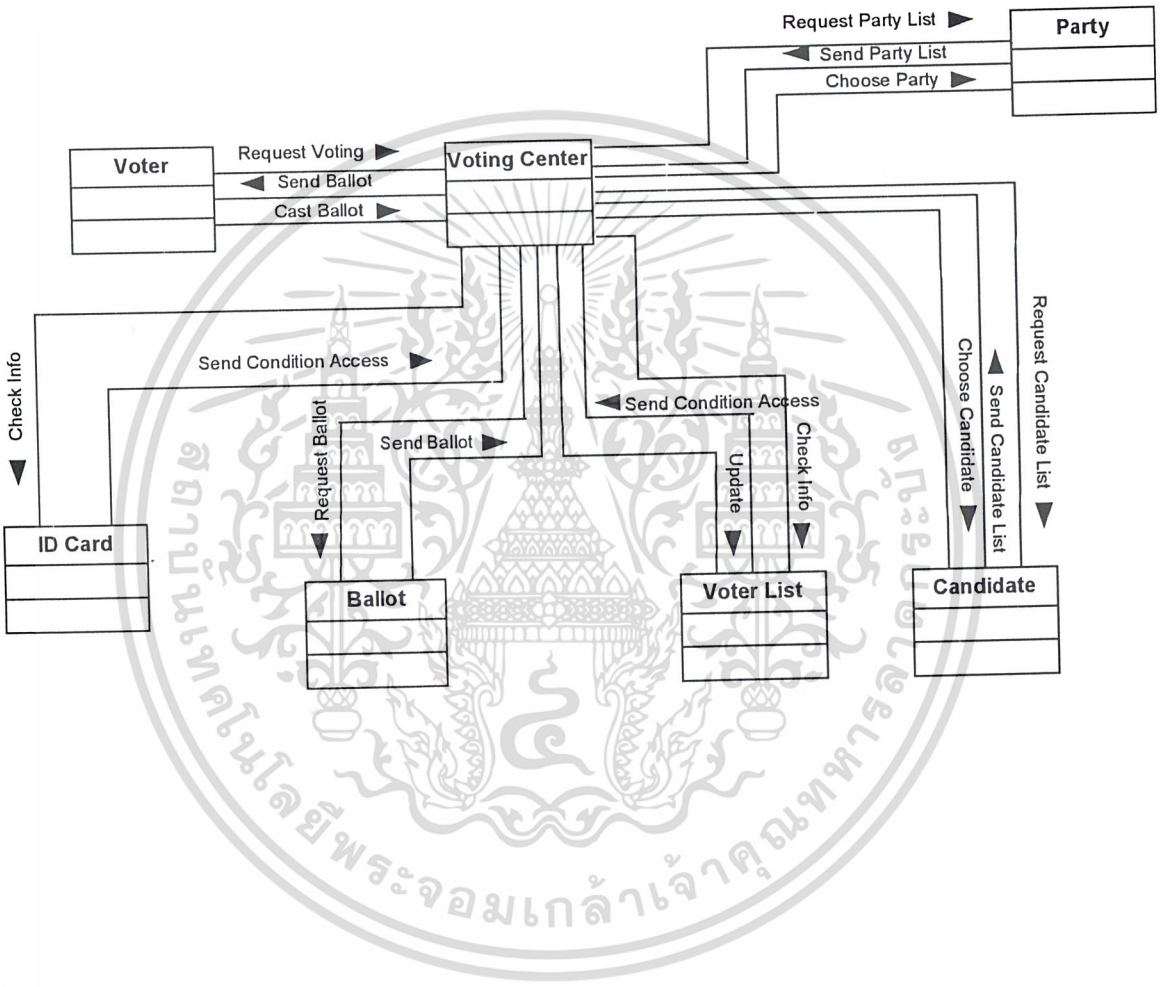


Activity Diagram (Continue)

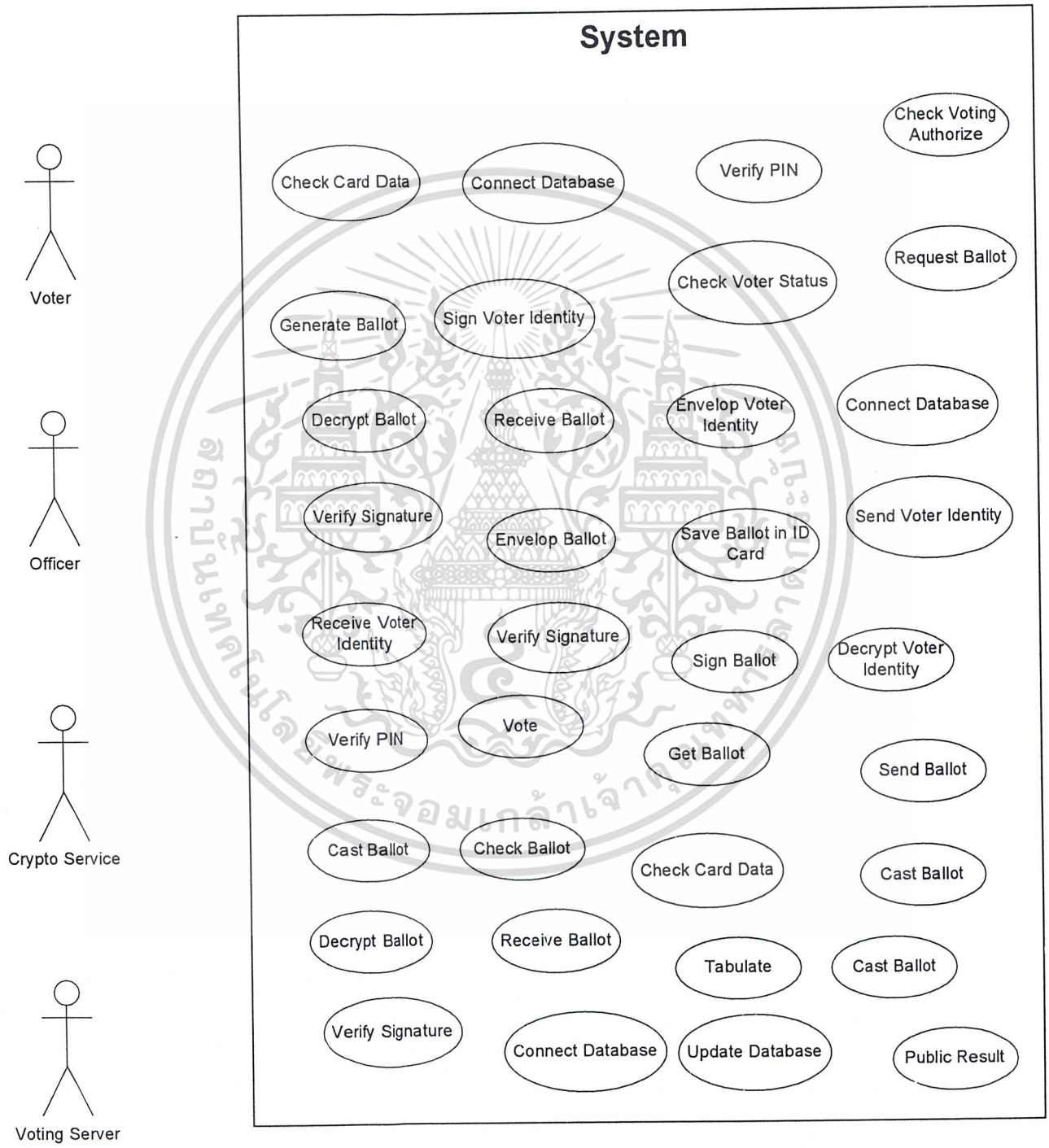


Voting Phase

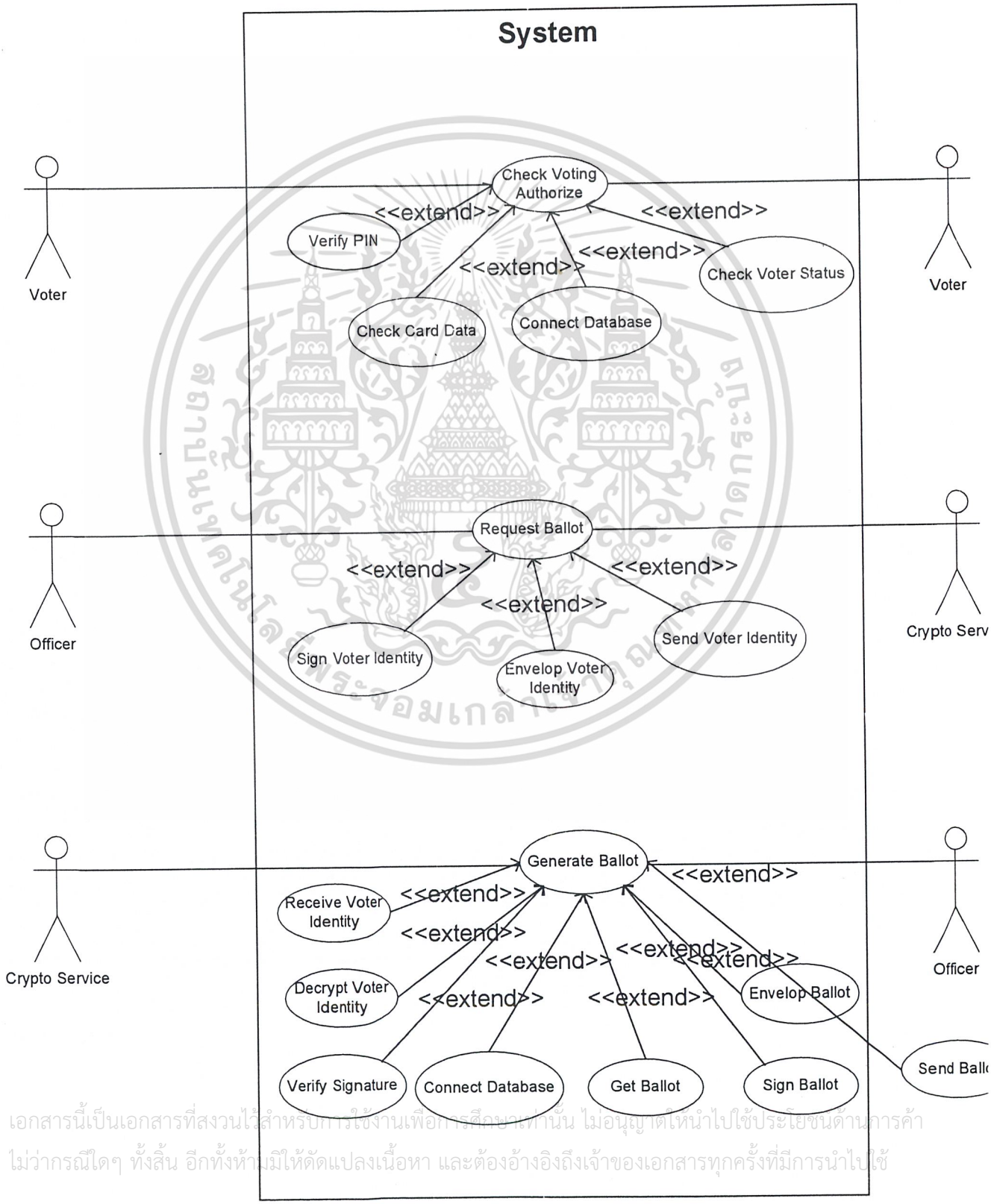
Client Interview



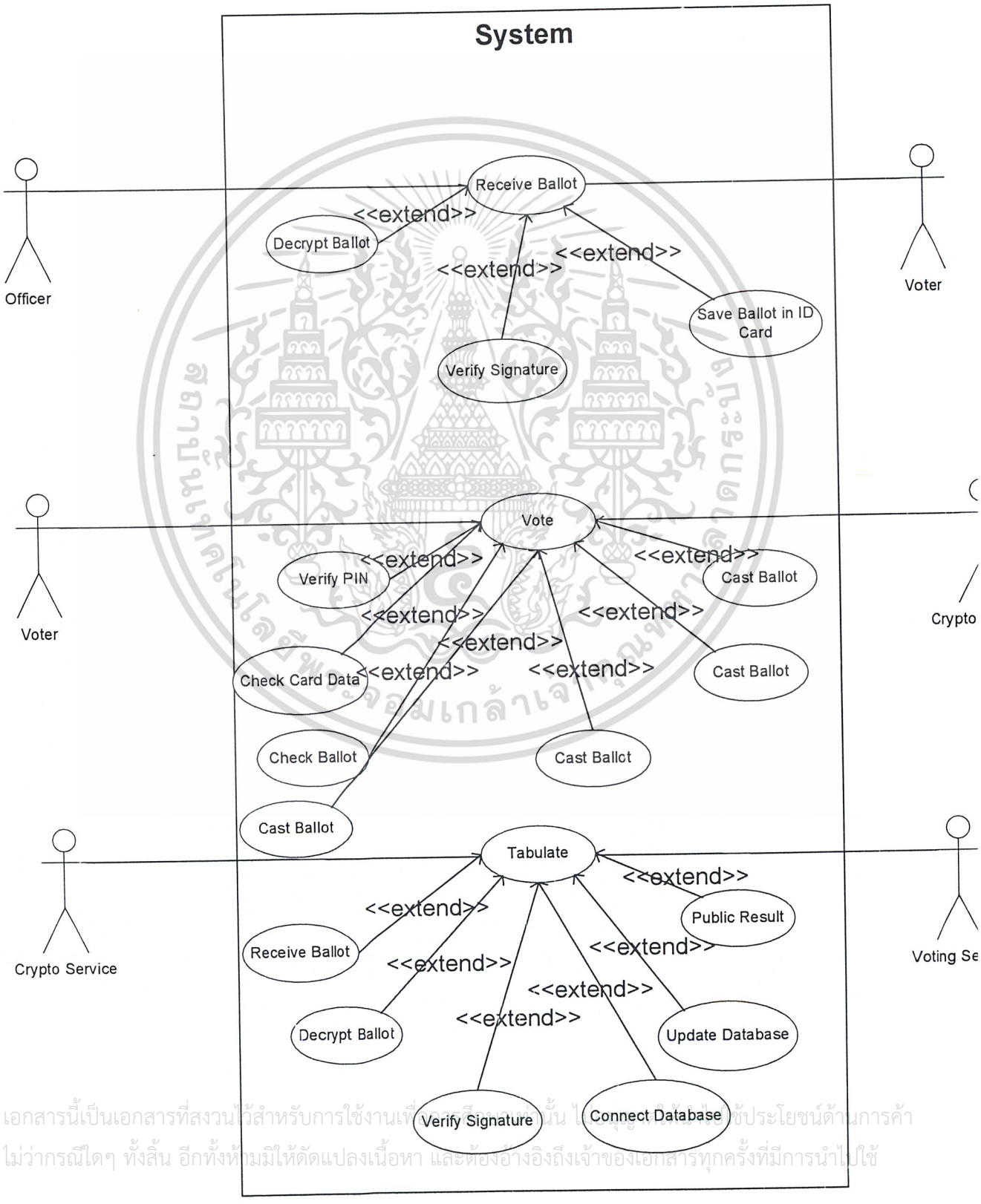
High Level Use Case



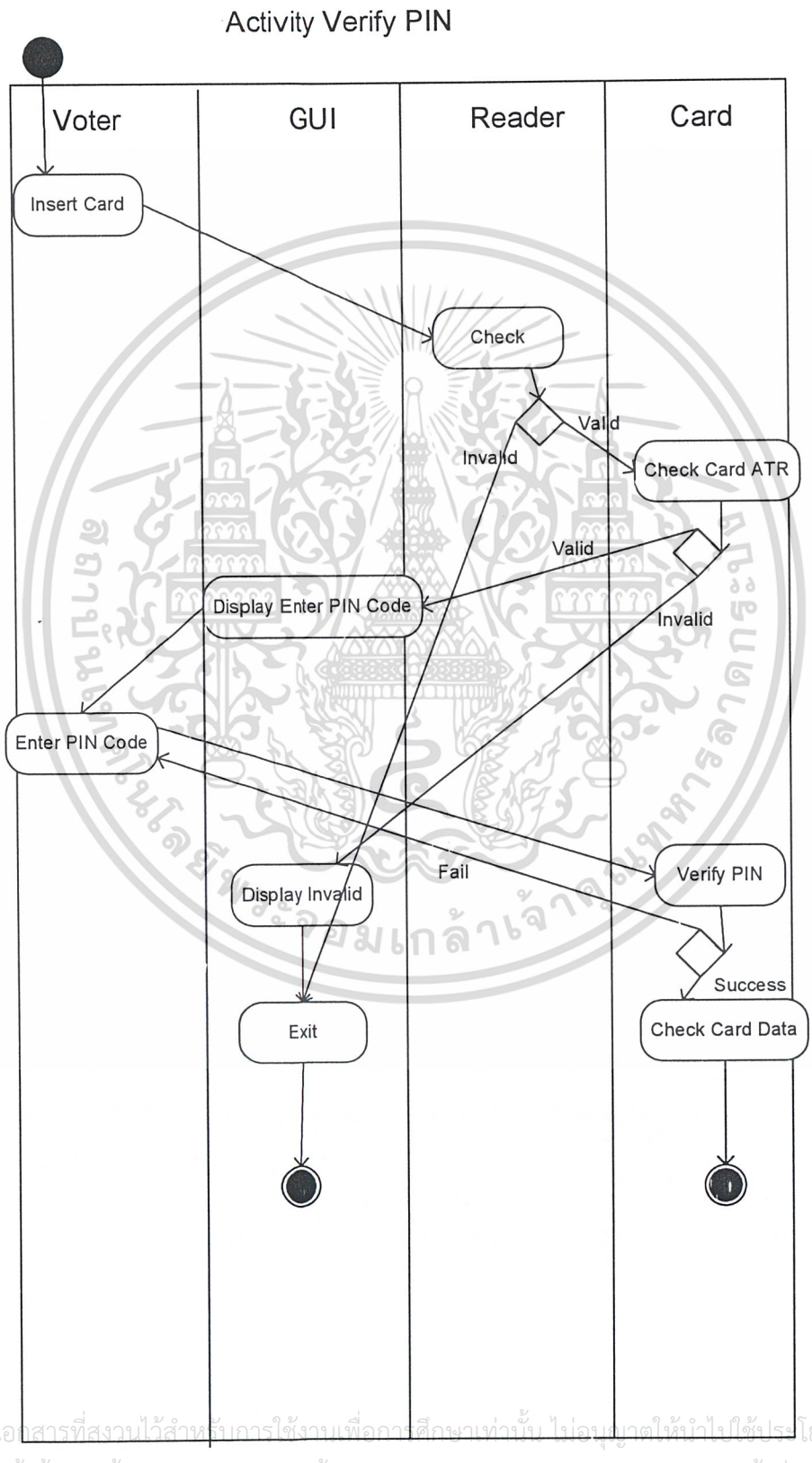
Use Case



Use Case (Continue)

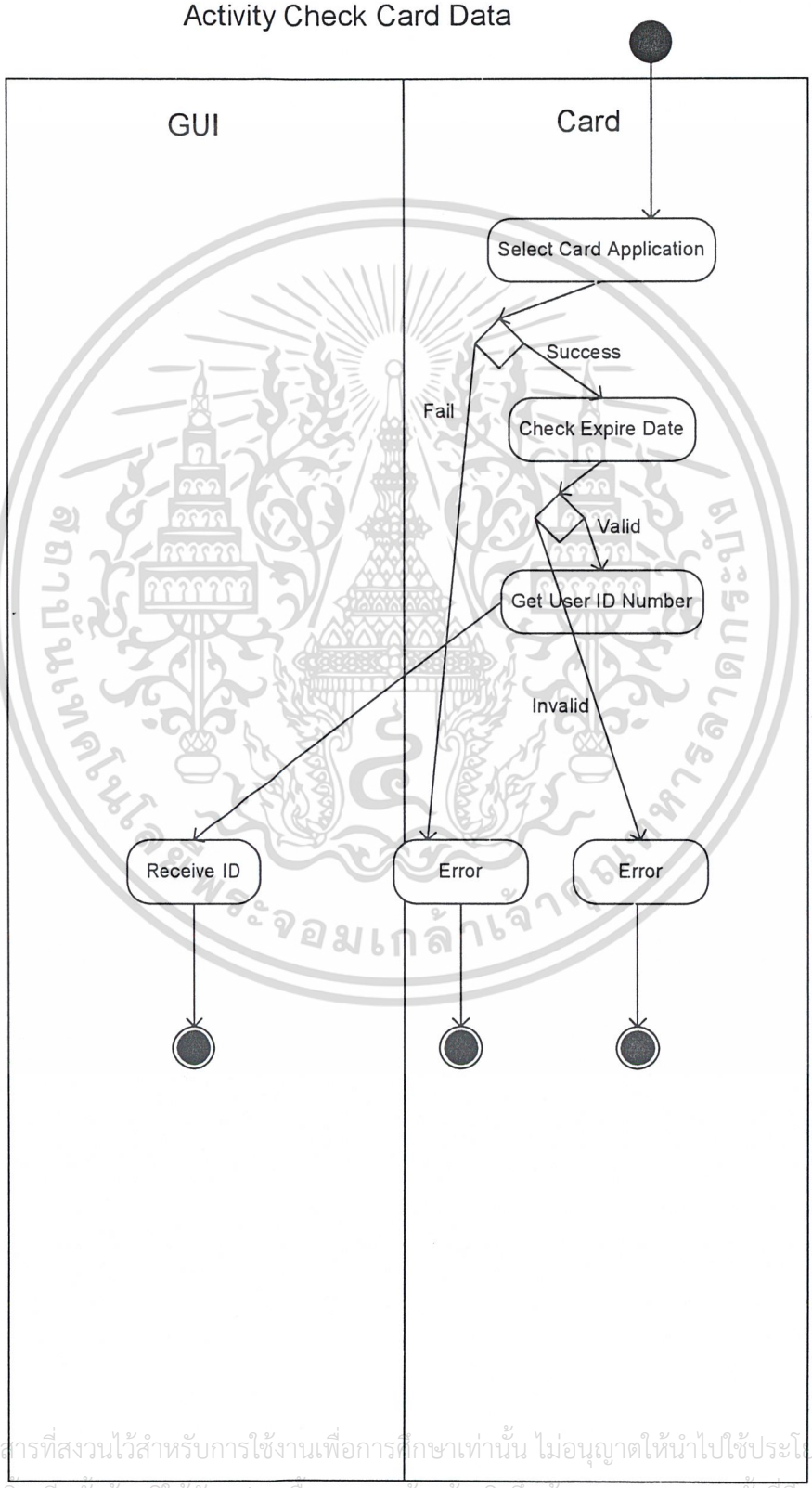


Activity Diagram

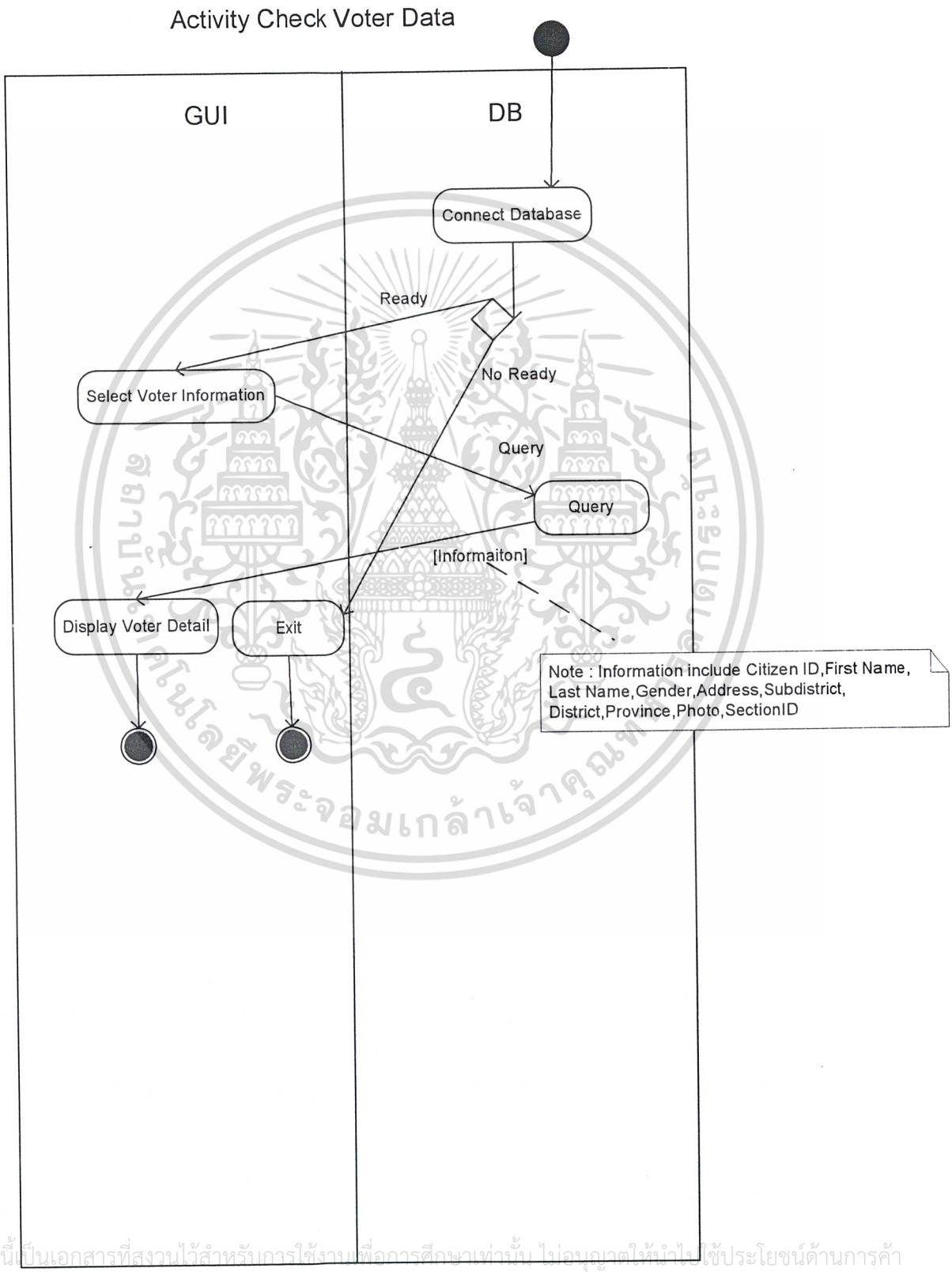


Activity Diagram (Continue)

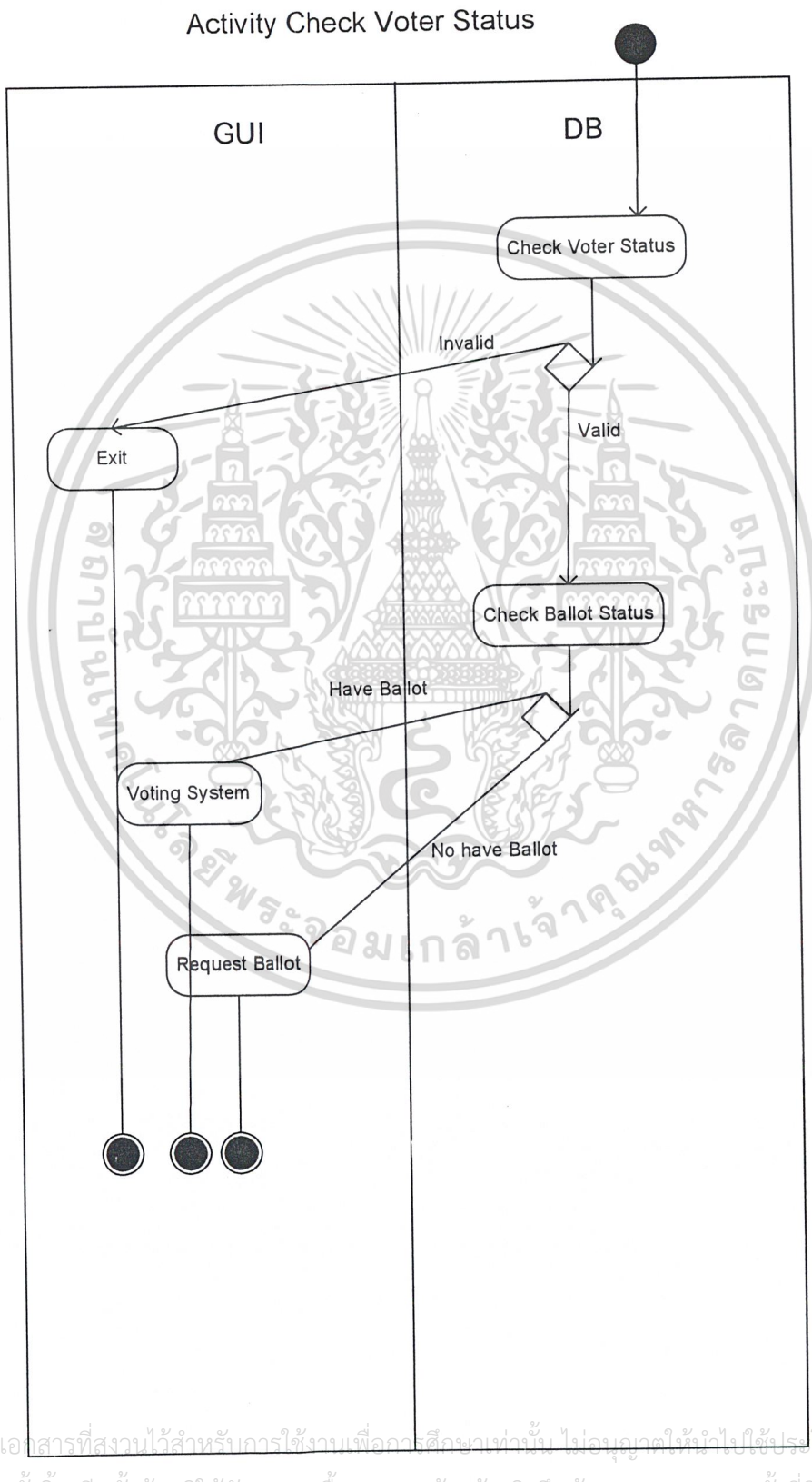
Activity Check Card Data



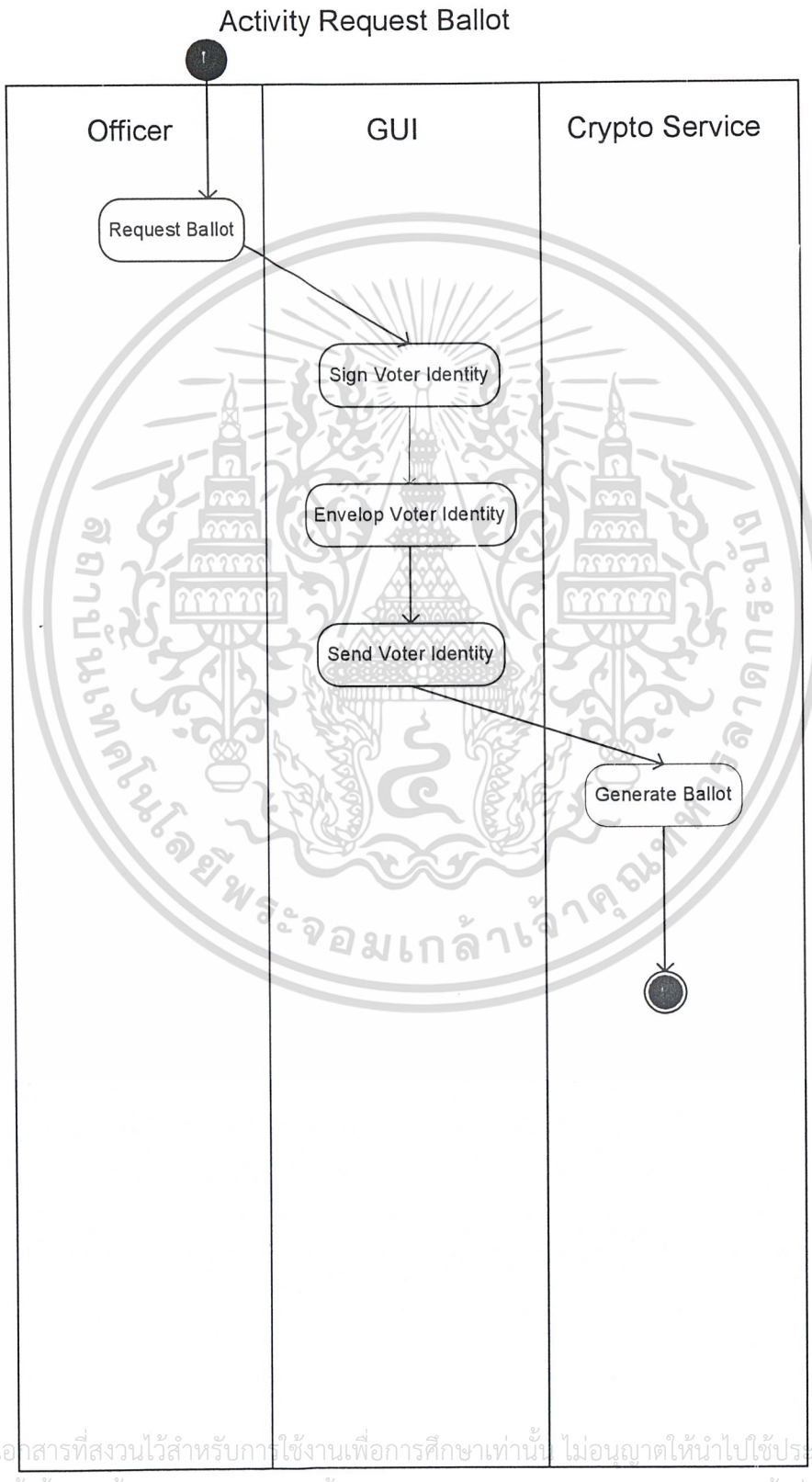
Activity Diagram (Continue)



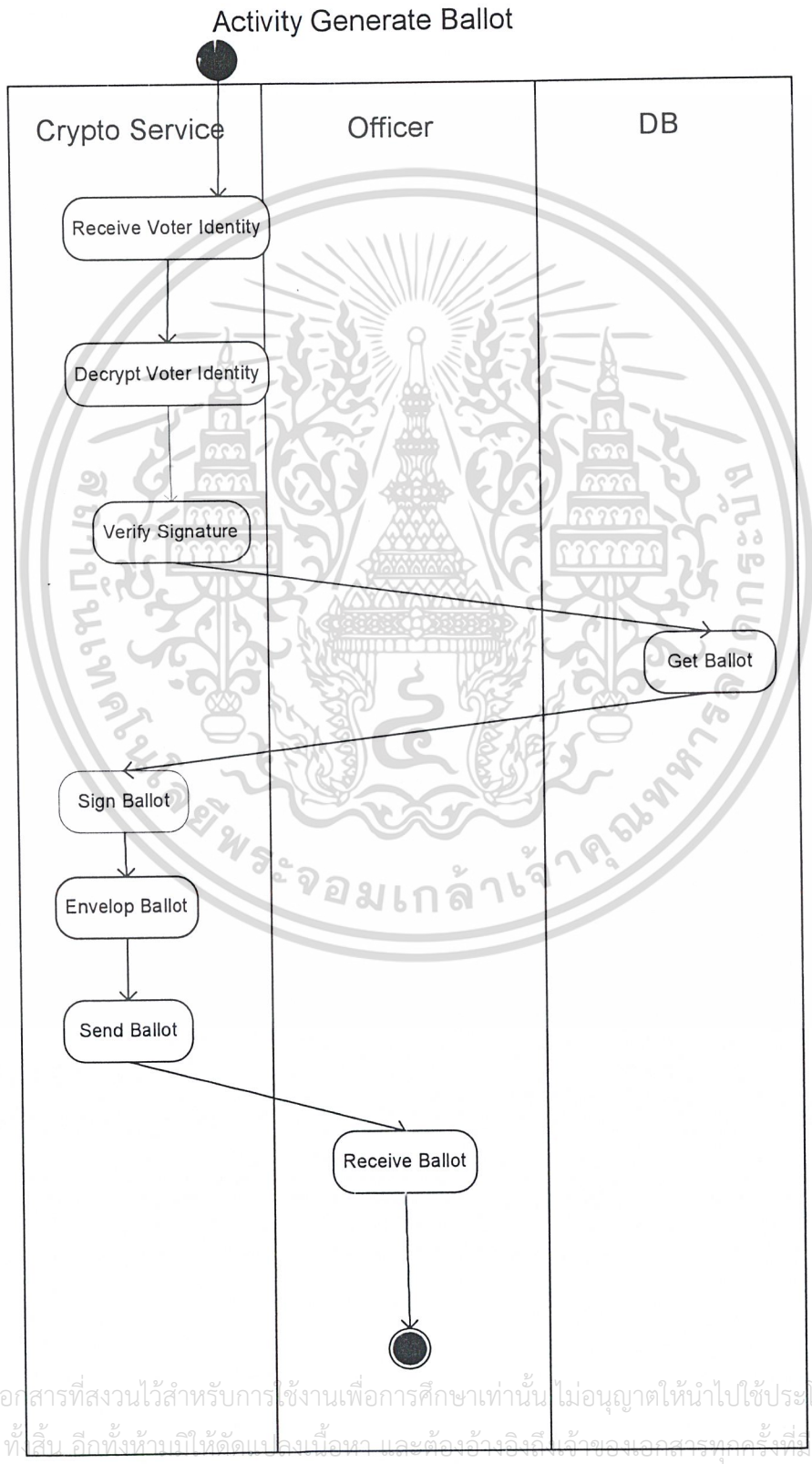
Activity Diagram (Continue)



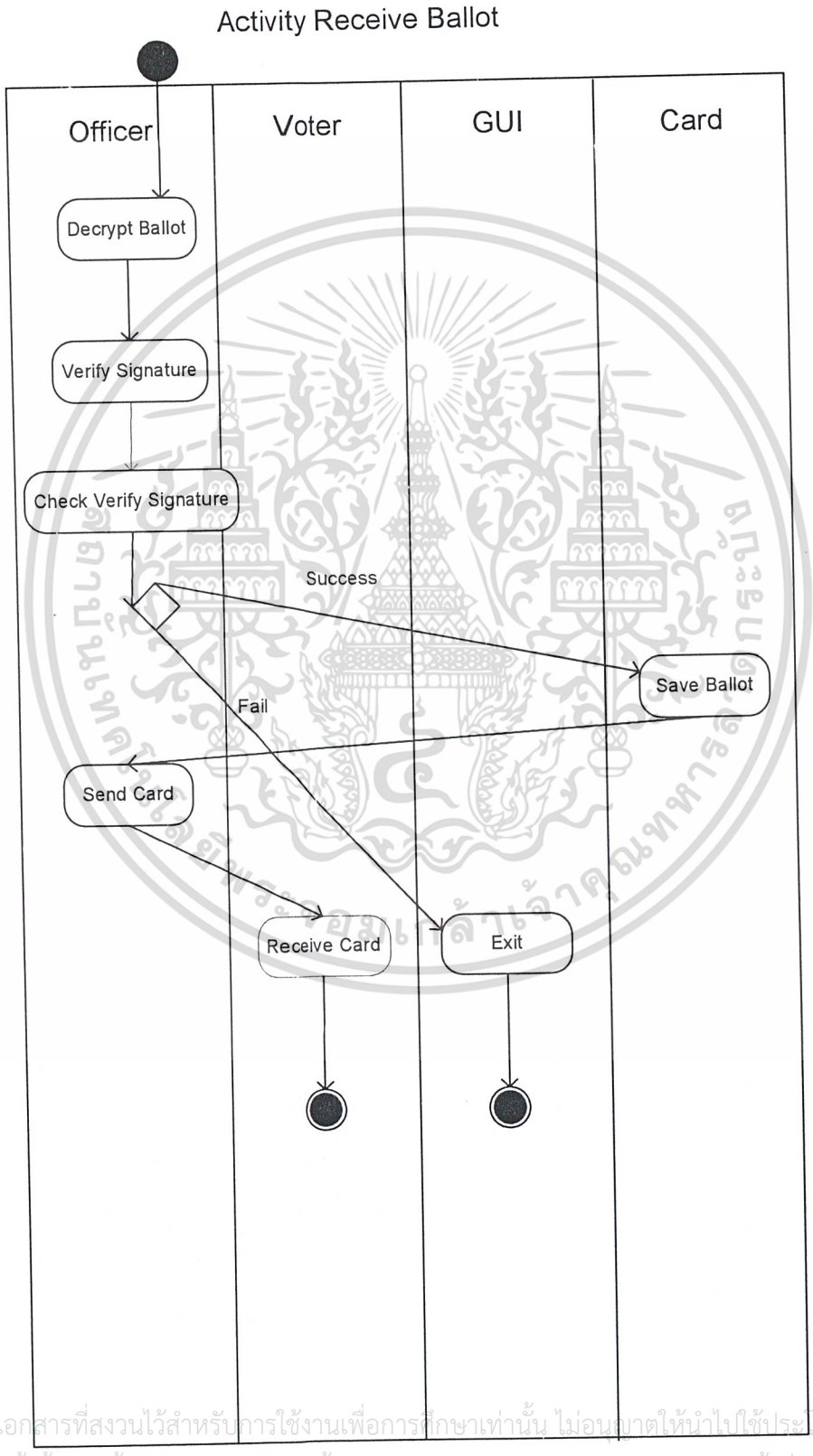
Activity Diagram (Continue)



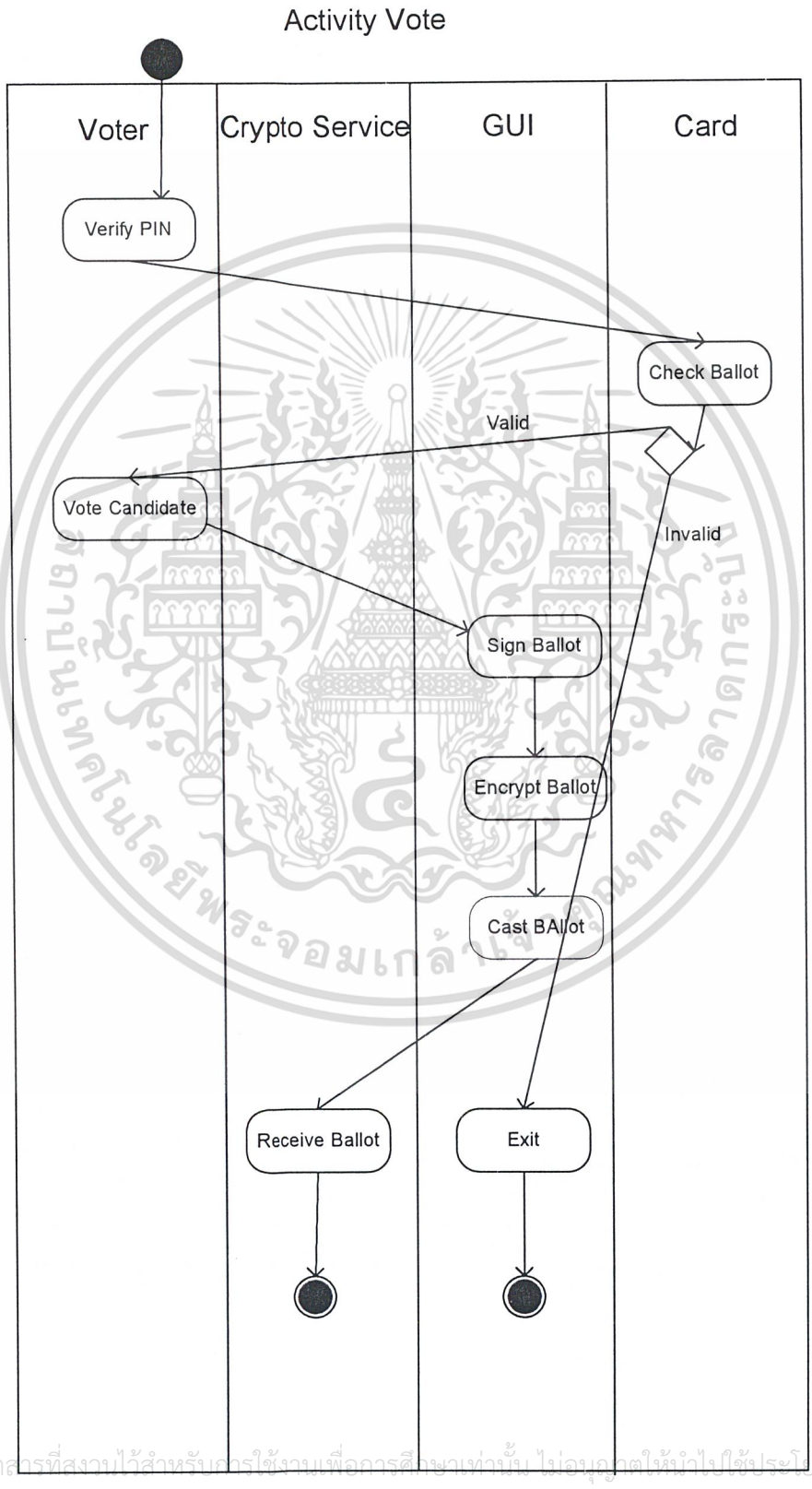
Activity Diagram (Continue)



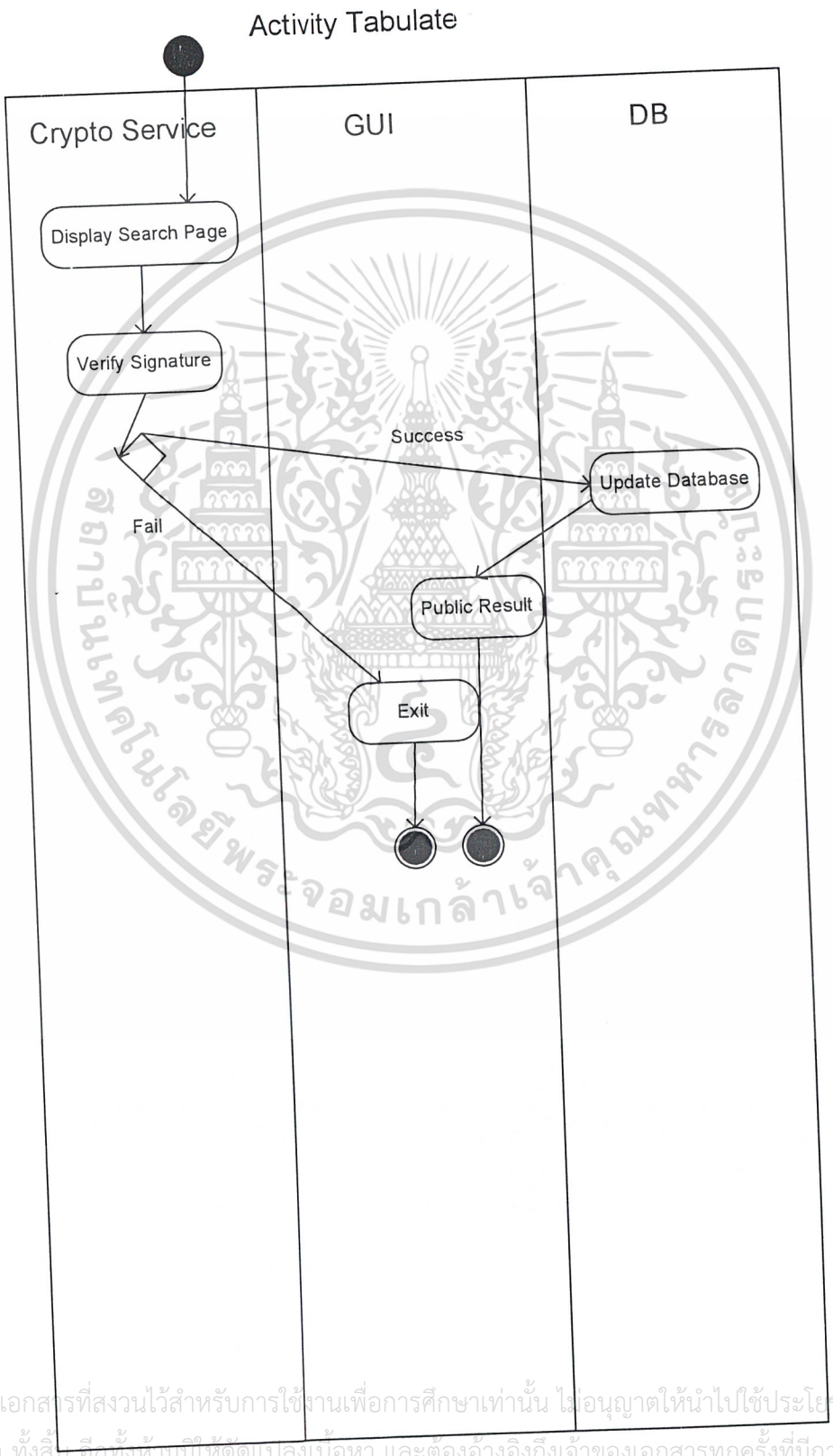
Activity Diagram (Continue)

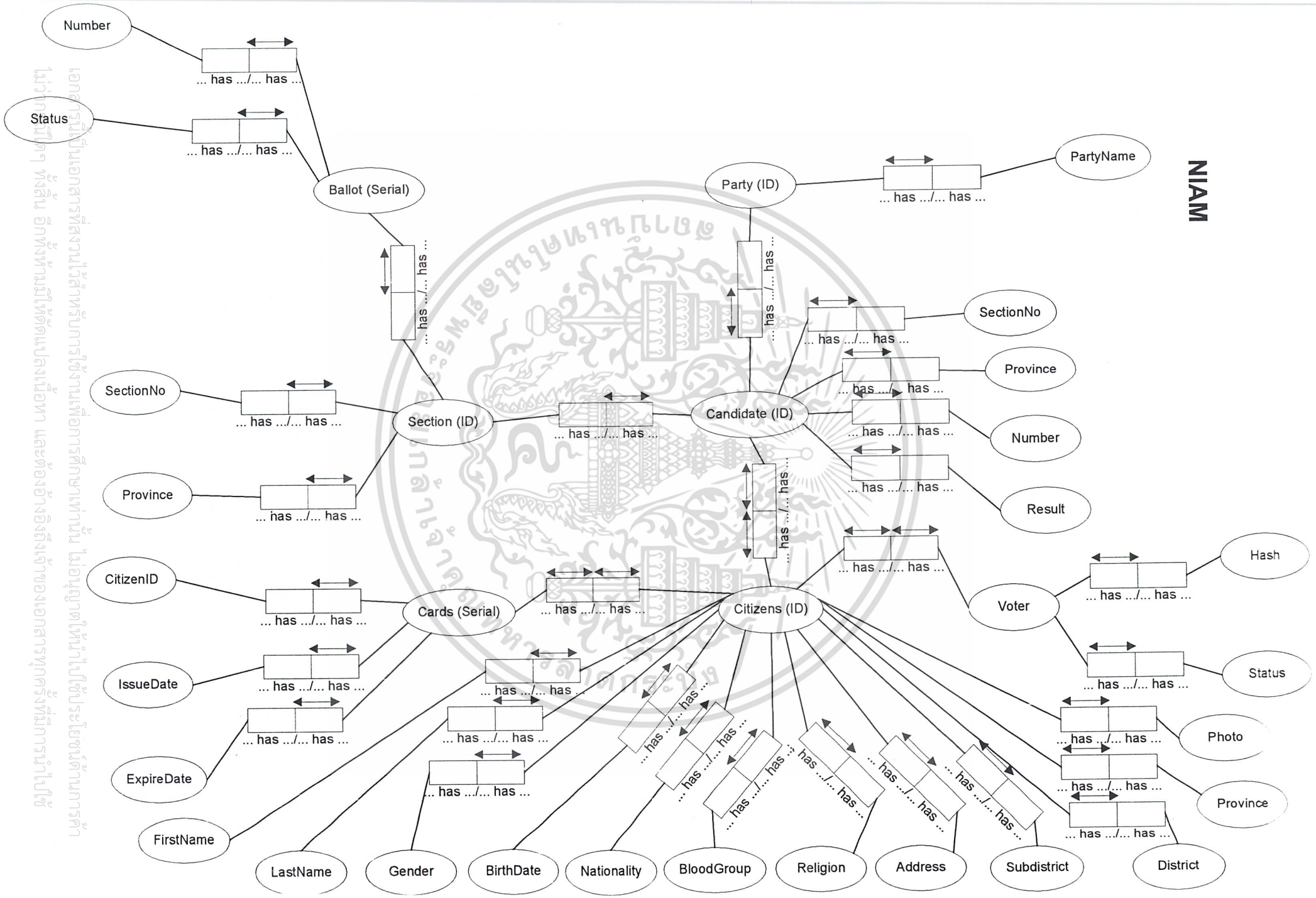


Activity Diagram (Continue)



Activity Diagram (Continue)




NIAM
Number
Status
Ballot (Serial)
... has .../... has ...
Party (ID)
PartyName
SectionNo
Province
Number
Result
Section (ID)
Candidate (ID)
CitizenID
Cards (Serial)
Citizens (ID)
Voter
Hash
Status
IssueDate
ExpireDate
FirstName
LastName
Gender
BirthDate
Nationality
BloodGroup
Religion
Address
Subdistrict
District
Photo

1. Citizens Table (ข้อมูลต่างๆของประชาชนตามบัตร)

Citizens (ID)	FirstName	LastName	Gender	Birthdate	Nationality	BloodGroup

Religion	Address	Subdistrict	District	Province	Photo

2. Voter Table (เก็บ Hash Function และสถานะการเลือกตั้งของผู้เลือกตั้ง)

Voter (ID)	Hash	Status

3. Cards Table (เก็บ Serial ของบัตร ,วันออกบัตร และวันหมดอายุของบัตร)

Cards (Serial)	Citizen (ID)	IssueDate	ExpireDate

4. Candidate Table (เก็บข้อมูลและผลคะแนนของผู้สมัคร)

Candidate (ID)	Party (ID)	SectionNo	Province	Number	Result

5. Party Table (เก็บรายชื่อพรรค)

Party (ID)	PartyName

6. Ballot Table (เก็บ Serial ของบัตรเลือกตั้ง ,สถานะของบัตร และผลการเลือก)

Ballot (Serial)	Section (ID)	Status	Number

7. Section Table (เก็บข้อมูลของเขตเลือกตั้ง)

Section (ID)	SectionNo	Subdistrict	District	Province

บรรณานุกรม

1. Java Card Technology Home Page. Http://java.sun.com/products/javacard/
2. Robin C. Townend. Finance, Smart Card News Ltd. http://www.smartcard.co.uk/
3. Smart Card Enhanced Security for Microsoft Windows 2000 System, Slumberger, http://www.cryptoflex.com/products/windows_2000/windows_2000.html
4. Zhiqun Chen, Java Card Technology for Smart Cards, 1 st Edition, ADDISON-WESLEY