การพัฒนาระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส

โดย

นายสมเกียรติ ดอนทองแดง

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาเทคโนโลยีสารสนเทศ

ภาควิชาคอมพิวเตอร์

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร

ปีการศึกษา 2551

การพัฒนาระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส

โดย

นายสมเกียรติ ดอนทองแดง

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาเทคโนโลยีสารสนเทศ

ภาควิชาคอมพิวเตอร์

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร

ปีการศึกษา 2551

DEVELOPMENT OF ACCESS CONTROL SYSTEM USING WEB SERVICE

By

Somkiat Dontongdang

An Independent Study Submitted in Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE

Department of Computing

Graduate School

SILPAKORN UNIVERSITY

2008

บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร อนุมัติให้การค้นคว้าอิสระเรื่อง “ การพัฒนาระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส ” เสนอโดย นายสมเกียรติ ดอนทองแดง เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

……..

(รองศาสตราจารย์ ดร.ศิริชัย ชินะตังกูร)

คณบดีบัณฑิตวิทยาลัย

วันที่.....เดือน..... พ.ศ.....

อาจารย์ที่ปรึกษาการค้นคว้าอิสระ

ผู้ช่วยศาสตราจารย์ ดร.ปานใจ ธารทัศนวงศ์

คณะกรรมการตรวจสอบการค้นคว้าอิสระ

..... ประธานกรรมการ

(อาจารย์ ดร.สุนีย์ พงษ์พินิจภิญโญ)

...../...../.....

..... กรรมการ

(อาจารย์ ดร.อาจิน จิรชีพพัฒนา)

...../...../.....

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.ปานใจ ธารทัศนวงศ์)

...../...../.....

48309326 : สาขาวิชาเทคโนโลยีสารสนเทศ
คำสำคัญ : เว็บเซอร์วิส ตรวจสอบบุคคล

สมเกียรติ ดอนทองแดง : การพัฒนาระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส. อาจารย์ที่ปรึกษาการค้นคว้าอิสระ : ผศ.ดร.ปานใจ ธารทัศนวงศ์. 87 หน้า.

การค้นคว้าอิสระครั้งนี้มีวัตถุประสงค์เพื่อ พัฒนาระบบการตรวจสอบบุคคลเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส เพื่อเพิ่มประสิทธิภาพให้กับระบบงานเดิม โดยนำเสนอกระบวนการการยืนยันตัวตนความเป็นเจ้าของบัตรด้วยลายนิ้วมือ เพื่อนำข้อมูลในบัตรไปใช้ในการเรียกใช้บริการข้อมูลต่างหน่วยงาน ผ่านเทคโนโลยีเว็บเซอร์วิส รวมทั้งการบันทึกรูปหน้าผู้เข้า-ออกสถานที่ลงฐานข้อมูล โดยผู้วิจัยได้ทำการจำลองระบบเว็บเซอร์วิสที่ให้บริการข้อมูลทั้งหมด 3 ระบบ คือ ระบบเว็บเซอร์วิสสำนักงานทะเบียนราษฎร์มีเซอร์วิส showdetail ที่ให้บริการข้อมูลประจำตัวประชาชน เพื่อใช้ในการเรียกใช้ข้อมูลประจำตัวประชาชนผู้ติดต่อ ระบบเว็บเซอร์วิสสำนักงานความมั่นคงแห่งชาติมีเซอร์วิส fileblacklist และระบบเว็บเซอร์วิสสำนักงานตำรวจแห่งชาติมีเซอร์วิส fileblacklist_police โดยทั้ง 2 ระบบทำหน้าที่ให้บริการข้อมูลผู้ต้องห้ามเข้าสถานที่ (Blacklist) เพื่อใช้ในการตรวจสอบข้อมูลผู้ติดต่อว่าเป็นผู้ต้องห้ามเข้าสถานที่หรือไม่

ผลของการค้นคว้าอิสระ แสดงให้เห็นว่า การนำบัตรประจำตัวประชาชนแบบสมาร์ทการ์ดมาใช้กับระบบ เพื่อทำการยืนยันตัวตน และการบันทึกรูปหน้าผู้เข้าสถานที่ลงฐานข้อมูล ได้ช่วยให้ข้อมูลมีความน่าเชื่อถือ ในการนำเทคโนโลยีเว็บเซอร์วิสมาใช้ เป็นเทคโนโลยีในการพัฒนาระบบ ช่วยให้หน่วยงานสามารถใช้บริการข้อมูล การตรวจสอบข้อมูลผู้ต้องห้ามเข้าสถานที่เป็นการช่วยลดความเสี่ยงในการเกิดความเสียหายกับสถานที่ จากผลการประเมินความพึงพอใจของผู้ทดสอบระบบ จำนวน 11 คน พบว่าในด้านการใช้งานระบบผู้ทดสอบระบบมีความพึงพอใจโดยมีค่าเฉลี่ยรวม เท่ากับ 3.61 และในด้านการทำงานของระบบผู้ทดสอบระบบมีความพึงพอใจโดยมีค่าเฉลี่ยรวม เท่ากับ 3.69 จากคะแนนความพึงพอใจของผู้ทดสอบระบบทั้ง 2 ด้าน แสดงให้เห็นว่า ผู้ทดสอบระบบมีความพึงพอใจต่อระบบในระดับที่ดี ดังนั้นผลของการค้นคว้าอิสระฉบับนี้ สามารถนำไปใช้เป็นแนวทางในการพัฒนาระบบการตรวจสอบบุคคลเข้า-ออกสถานที่ เพื่อให้เกิดประโยชน์สูงสุด

ภาควิชาคอมพิวเตอร์ บัณฑิตวิทยาลัย มหาวิทยาลัยศิลปากร ปีการศึกษา 2551
ลายมือชื่อนักศึกษา.....
ลายมือชื่ออาจารย์ที่ปรึกษาการค้นคว้าอิสระ .....

48309326 : MAJOR : INFORMATION TECHNOLOGY
KEY WORD : WEB SERVICE SMART CARD
SOMKIAT DONTONGDANG : DEVELOPMENT OF ACCESS CONTROL SYSTEM USING WEB SERVICE. INDEPENDENT STUDY ADVISOR : ASST.PROF. PANJAI TANTATSANAWONG, Ph.D. 87 pp.

The independent study proposed the development of access control system using Web Service to increase the efficiency of the former system. In this study, the process was presented by confirming the fingerprint of owner card. It was able to take the organization data by using Web Service technology and record the face of visitors who enter in that organization on the database. Three systems were simulated using the Web Service. The first was the showdetail Web Service system about the identification of visitors that can retrieve the data of them by linking to the Civil Registration Session. The second was the fileblacklist Web Service system in the Security Council and the last was the fileblacklist_police Web Service system in the Royal Thai Police. Both organizations used Web Service system for giving blacklist data to detect visitors who contact with these places.

The results of this study indicated that using smart card in this system to identify visitors and record the faces of them on the database. These helped to increase data reliability, Web Service technology used to develop the system in the organization in order to transfer backlist visitor's data to the local database. This system can enhance the security and stability in the organization. The assessment of eleven users found that they satisfied in this system by giving satisfied the mean of score 3.61 and the mean of satisfied score in working system was 3.69. These scores indicated that users had satisfaction in both systems at a good level. Therefore, the end results of this independent study are that promote the benefit of the development of access control system.

Department of Computing Graduate School, Silpakorn University Academic Year 2008
Student's signature .....
Independent Study Advisor's signature .....

กิตติกรรมประกาศ

การค้นคว้าอิสระฉบับนี้ได้ด้วยความกรุณาให้คำปรึกษาแนะนำช่วยเหลืออย่างดียิ่งจาก ผู้ช่วยศาสตราจารย์ ดร.ปานใจ ธารทัศนวงศ์ ดร.สุนีย์ พงษ์พินิจภิญโญ จนสำเร็จเรียบร้อย ถูกต้องและสมบูรณ์ ผู้วิจัยขอกราบขอบพระคุณด้วยความซาบซึ้งใจไว้ ณ โอกาสนี้และขอกราบขอบพระคุณคณาจารย์ประจำภาควิชาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยศิลปากรทุกท่านที่ประสิทธิ์ประสาทวิชาให้อย่างเต็มความสามารถ ขอขอบคุณพี่ ๆ เพื่อน ๆ ทุกคนที่ให้ความช่วยเหลือและเป็นกำลังใจ

สุดท้ายนี้ ต้องขอบพระคุณคุณพ่อและคุณแม่ ที่คอยสนับสนุน คอยให้กำลังใจและเป็นแรงผลักดันให้ผู้วิจัยได้ศึกษาต่อจนสำเร็จการศึกษา ประโยชน์ และคุณค่าใด ๆ อันเกิดจากการค้นคว้าอิสระฉบับนี้ ผู้วิจัยขอน้อมนำบูชาแด่พระคุณ บิดา มารดา บูรพาจารย์ ผู้ให้แสงสว่างแห่งปัญญาและขอมอบเป็นรางวัลแด่ครอบครัว ดอนทองแดง ทุกคน

สารบัญ

บทที่ หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญภาพ

ภาพที่ หน้า

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

มีเหตุการณ์ความไม่สงบที่เกิดขึ้นบ่อยครั้งในปัจจุบัน ก่อให้เกิดความเสียหายหลายด้าน และมีหลายเหตุการณ์ความไม่สงบที่เกิดขึ้นแล้วไม่สามารถรู้ได้เป็นการกระทำของใคร สาเหตุเนื่องมาจาก ไม่มีข้อมูลที่ระบุได้ว่าใครเป็นผู้กระทำ แต่ทางเลือกที่ดีที่สุดก็คือการป้องกันมิให้เกิดความเสียหายนั้นขึ้น โดยมีการพัฒนาระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส ในการแสดงข้อมูลของผู้ต้องการติดต่อเข้าสถานที่ และมีการยืนยันตัวตนการเป็นเจ้าของบัตร โดยใช้ลายนิ้วมือในการเปรียบเทียบ เพื่อให้ระบบมีความปลอดภัยและมีความน่าเชื่อถือ จึงต้องมีการตรวจสอบข้อมูลของผู้ติดต่อเข้าสถานที่ ว่าเป็นบุคคลที่มีชื่ออยู่ใน Blacklist หรือไม่ โดยมีการแลกเปลี่ยนข้อมูลระหว่างองค์กรบนระบบอินเทอร์เน็ต ด้วยเทคโนโลยีเว็บเซอร์วิส ในการติดต่อกันระหว่างองค์กร ซึ่งมีความแตกต่างกันระหว่างแอพพลิเคชั่นที่ถูกพัฒนามาจากหลายหลายแพลตฟอร์ม และหลากหลายภาษา ถึงแม้ว่าองค์กรต่าง ๆ สามารถเชื่อมแอพพลิเคชั่นต่าง ๆ เข้าด้วยกันได้ แต่การทำเช่นนี้ มีค่าใช้จ่ายสูง และมีความสลับซับซ้อนมาก ด้วยเหตุนี้จึงจำเป็นต้องมีมาตรฐานกลางในการติดต่อเพื่อให้การติดต่อสื่อสาร และการทำงานร่วมกันระหว่างองค์กรง่ายขึ้น และรวดเร็วมากขึ้น โดยมาตรฐานกลางที่ว่านั้น คือ เว็บเซอร์วิส

วัตถุประสงค์

1. ศึกษาและพัฒนาระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส
2. ประเมินผลระบบที่พัฒนาขึ้น

ขอบเขตการวิจัย

1. ศึกษาเทคโนโลยีบัตรประชาชนสมาร์ทการ์ด, การสแกนลายนิ้วมือ, เว็บเซอร์วิส และการ capture ภาพจากกล้อง Webcam บันทึกลงฐานข้อมูล

2. จำลองเว็บเซอร์วิสที่เปิดให้บริการข้อมูลได้แก่ ระบบเว็บเซอร์วิสสำนักงานตำรวจแห่งชาติ ระบบเว็บเซอร์วิสสำนักงานความมั่นคงแห่งชาติ และระบบเว็บเซอร์วิสสำนักงานทะเบียนราษฎร์

3. วิเคราะห์และออกแบบระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส

ขั้นตอนในการสร้างและพัฒนาระบบ

1. สร้างระบบเชื่อมต่อระหว่างระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิสกับระบบการบริการข้อมูลผู้ที่มีรายชื่อในBlacklist เพื่อใช้ในการค้นหา เปรียบเทียบ และแสดงข้อมูล
2. ศึกษาการใช้เครื่องอ่านบัตรประชาชนแบบสมาร์ทการ์ด และการสแกนลายนิ้วมือ
3. ศึกษาเทคโนโลยีการ Capture ภาพจากกล้อง Webcam บันทึกลงฐานข้อมูล
4. จำลองเว็บเซอร์วิสที่ให้บริการข้อมูลได้แก่ ระบบเว็บเซอร์วิสสำนักงานตำรวจแห่งชาติ ระบบเว็บเซอร์วิสสำนักงานความมั่นคงแห่งชาติ และระบบเว็บเซอร์วิสสำนักงานทะเบียนราษฎร์

ผลที่คาดว่าจะได้รับ

1. ระบบสามารถรองรับการใช้งานได้อย่างมีประสิทธิภาพ และมีความน่าเชื่อถือ
2. ระบบสามารถยืนยันตัวบุคคลในความเป็นเจ้าของบัตร
3. มีการแลกเปลี่ยนข้อมูลกันระหว่างองค์กรในรูปแบบเว็บเซอร์วิส
4. ระบบมีการเตือนเมื่อมีบุคคลที่ติดต่อเข้าสถานที่ตรงกับข้อมูล Blacklist
5. ระบบสามารถเก็บบันทึกข้อมูลรูปหน้าผู้ติดต่อและเรียกใช้ได้

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ทฤษฎีที่เกี่ยวข้อง

1. ระบบบัตรประจำตัวประชาชนแบบสมาร์ทการ์ด (Smart Card) (สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการสถาบันวิจัยและให้คำปรึกษาแห่ง มหาวิทยาลัยธรรมศาสตร์/ TU-RAC 2547 : 23 - 47)

บัตรสมาร์ทการ์ด คือ ชื่อเรียกของเทคโนโลยีในการทำบัตรพลาสติกที่มีขนาดเท่ากับบัตรเครดิตหรือบัตรเอทีเอ็ม ซึ่งมีการฝังชิพ (Chip) ไว้ภายในบัตร ชิพดังกล่าวจะเป็นที่เก็บข้อมูลต่าง ๆ จำนวนมากในรูปแบบอิเล็กทรอนิกส์ซึ่งจุดที่แตกต่างจากเทคโนโลยีบัตรแถบแม่เหล็กที่ใช้กันแต่เดิม โดยบัตรสมาร์ทการ์ดสามารถบรรจุข้อมูลได้มากกว่าบัตรแถบแม่เหล็กธรรมดาถึง 100 เท่า

1.1 ระบบของบัตรสมาร์ทการ์ด ที่ใช้อยู่ในปัจจุบันสามารถแบ่งออกได้เป็น 2 แบบใหญ่ ๆ คือ

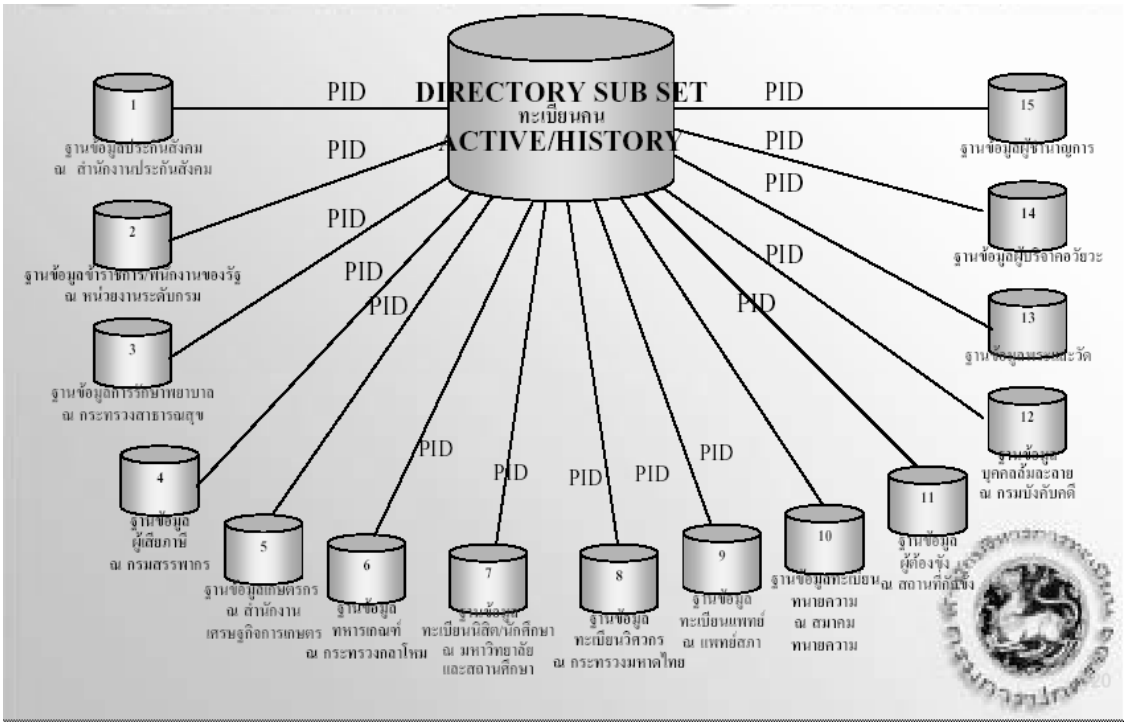
1.1.1 สมาร์ทการ์ดแบบมีการสัมผัส (Contact smart cards) ซึ่งการใช้งานจำเป็นต้องมีการสอดใส่เข้าไปในเครื่องอ่านสมาร์ทการ์ด (Smart cards reader) สมาร์ทการ์ดแบบ มีการสัมผัสเป็นบัตรที่มีการผนึกชิพทองขนาดเล็กเส้นผ่าศูนย์กลางประมาณครึ่งนิ้วไว้ที่ด้านหน้าบัตรแทนการใช้แถบแม่เหล็ก (Magnetic stripe) ที่เคยพบเห็นใช้กันมากที่สุดในบัตรเครดิตหรือบัตรเอทีเอ็ม เมื่อผู้ใช้สอดใส่บัตรเข้าไปในเครื่องอ่านบัตรสมาร์ทการ์ดแล้ว มันจะสัมผัสกับหัวต่อ (connecter) ทางไฟฟ้าซึ่งจะทำการส่งถ่ายข้อมูลเข้าและออกจากชิพ

1.1.2 สมาร์ทการ์ดแบบไม่มีสัมผัส (Contactless smart card) ซึ่งในการใช้งานต้องการเพียงให้วางอยู่ใกล้ ๆ กับสายอากาศเท่านั้น สมาร์ทการ์ดแบบไม่มีการสัมผัสเป็นบัตรที่มองดูรูปร่างภายนอกแล้วคล้ายกับบัตรเครดิตพลาสติกแบบหนึ่งที่ภายในมีการผนึกชิพคอมพิวเตอร์และขดลวดสายอากาศไว้ภายใน ซึ่งใช้ในการติดต่อกับเครื่องรับ/เครื่องส่งที่อยู่ในระยะไกล (Remote receive/ transmitter) โดยทั่ว ๆ ไปเรามักใช้บัตรแบบนี้ เมื่อต้องมีการดำเนินการทางด้านรายการ (Transactions) อย่างรวดเร็วตัวอย่างเช่นบัตรที่ใช้กับการจัดเก็บเงินค่าทางด่วน

นอกจากบัตรสมาร์ทการ์ดทั้งสองแบบดังกล่าวแล้ว ปัจจุบันยังมีการผลิตสมาร์ทการ์ดแบบผสมหรือที่เรียกว่า คอมบิ การ์ด (Combi-Card) ออกมาใช้งานอีกด้วย โดยบัตรแบบนี้เป็นบัตรใบเดียวแต่ทำหน้าที่เป็นทั้งสมาร์ทการ์ดแบบมีการสัมผัส และสมาร์ทการ์ดแบบไม่มีการสัมผัส เพื่อเพิ่มความสะดวกและประโยชน์ในการใช้งานมากขึ้น

ดังนั้นบัตรประจำตัวประชาชนแบบสมาร์ทการ์ด จึงเป็นบัตรประชาชนรุ่นใหม่ที่ใช้เทคโนโลยีดังกล่าวมาใช้แทนทำบัตรประชาชนที่ใช้เทคโนโลยีบัตรแถบแม่เหล็ก กล่าวคือเป็นบัตรประจำตัวประชาชนที่ใช้แสดงตนที่มีชิพ สามารถบันทึกข้อมูลบุคคล ของทางราชการรวมทั้งข้อมูลส่วนบุคคลของผู้ถือบัตรที่ผู้ถือบัตรยินยอม และใช้เป็นกุญแจมาตรฐานในการเข้าถึงข้อมูลของส่วนราชการที่เกี่ยวข้องกับตน ตลอดจนสามารถใช้ขอเข้ารับบริการจากทุกหน่วยงานในวันนี้หรือในอนาคต เพื่อความรวดเร็วในการให้บริการและลดขั้นตอนการทำงานและเอกสารของทางราชการ

สำหรับความแตกต่างระหว่างการจัดทำบัตรประจำตัวประชาชนแบบเดิม (ติดรูปถ่าย) และบัตรสมาร์ทการ์ดนั้น อยู่ที่บัตรประจำตัวประชาชนระบบเดิม (ติดรูปถ่ายด้วยมือ) เป็นการจัดทำบัตรแบบรวมศูนย์ทำที่ส่วนกลาง (Centralization) และทำด้วยมือ ทำให้ต้องใช้เวลานานกว่าประชาชนจะได้รับบัตร รวมทั้งทำการปลอมแปลงได้ง่ายแต่บัตรประจำตัวประชาชนแบบสมาร์ทการ์ดเป็นการจัดทำบัตรระบบกระจายการทำบัตรไปยังสำนักงานทะเบียน (Decentralization) และใช้ระบบอิเล็กทรอนิกส์ ทำให้ประชาชนได้รับบัตรรวดเร็วขึ้น ขอทำบัตรที่สำนักทะเบียนแห่งก็ได้ และ จะได้รับบัตรทันที ภายใน 15 นาที ปลอมแปลงยาก และง่ายต่อการใช้ประโยชน์ ซึ่งชิพ จะเป็นหัวใจสำคัญของการเก็บข้อมูลในบัตรประจำตัวประชาชนแบบสมาร์ทการ์ดนี้ดังภาพที่ 1



ภาพที่ 1 แสดงแหล่งข้อมูลบัตรประจำตัวประชาชนแบบสมาร์ทการ์ด
ที่มา : สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์/ TU-RAC, การคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในบัตรประจำตัวแบบสมาร์ทการ์ด (Smart Card), (ม.ป.ท., 2547), 34

โดยรัฐบาลมีวัตถุประสงค์ที่จะใช้บัตรสมาร์ทการ์ดเป็นบัตรหลักบัตรเดียว เพื่อใช้บริการได้ทุกหน่วยงานราชการและหน่วยงานต่าง ๆ เช่นการประกันสุขภาพ การประกันสังคม และสามารถใช้ร่วมกับบริการของธนาคารเป็นบัตร ATM บัตรเครดิต บัตรเติมเงินสดหรือชำระราคาสินค้าได้ในอนาคต ซึ่งการใช้บัตรดังกล่าวมีวิธีการใช้ที่สะดวกและปลอดภัยสูง เพียงแค่นำบัตรป้อนเข้าเครื่องอ่านบัตร ประทับลายพิมพ์นิ้วมือหรือใส่รหัส PIN (Personal Identification Number) เพื่อยืนยันการอนุญาตจากเจ้าของบัตร

1.2 ประโยชน์ของบัตรประจำตัวประชาชนแบบสมาร์ทการ์ด

บัตรประจำตัวประชาชนแบบสมาร์ทการ์ดนี้มีประโยชน์ทั้งต่อหน่วยงานภาครัฐและภาคประชาชนหลายประการ ได้แก่

1.2.1 ประโยชน์ต่อหน่วยงานภาครัฐ จะเป็นการลดขั้นตอนที่ซ้ำซ้อนของการทำบัตรของหน่วยงานภาครัฐเป็นการใช้ทรัพยากรของหน่วยงานร่วมกันและประหยัดงบประมาณประเทศ

1.2.2 ประโยชน์ต่อประชาชน จะเป็นการประหยัดเวลาในการจัดทำบัตรซึ่งเดิมใช้เวลา 3 เดือน เหลือ 15 นาที การยืนยันตัวบุคคลเพื่อเข้าสู่ระบบบริการแบบอิเล็กทรอนิกส์ของภาครัฐหรือเอกชนที่จะเข้าร่วมและจะได้รับบริการภาครัฐที่ครบถ้วนมากขึ้น โดยใช้บัตรเพียงใบเดียว ทั้งนี้ก็ยังมีประโยชน์ของบัตรอื่น ๆ คือ ใช้บริการ E-mail และธุรกรรมอิเล็กทรอนิกส์ของภาครัฐในระยะแรก ใช้บัตรลงทะเบียน เพื่อขอรับการบริการของภาครัฐ ที่รวดเร็ว สะดวกและปลอดภัยสูง ใช้บัตรขอรับบริการด้านการสาธารณสุขตามโครงการหลักประกันสุขภาพ (30 บาทรักษาทุกโรค) ใช้บัตรเพื่อขอรับบริการด้านการประกันสังคม,ใช้บัตรเพื่อการปฏิบัติงานการเข้าถึงข้อมูลที่ต้องเกี่ยวข้องกับการรักษาความปลอดภัย ระดับสูงของภาครัฐ, ใช้เป็นบัตรแทนบัตรประจำตัวเจ้าหน้าที่ของรัฐ ที่มีการปลอมแปลงได้ยาก,ใช้ตรวจสอบข้อมูลการทะเบียนของประชาชนแบบ On-Line เฉพาะบุคคลได้ และอนาคตสามารถใช้เป็นบัตรเพื่อลงประชามติหรือการเลือกตั้ง ตลอดจนใช้เป็นบัตรแทนใบขับขี่รถยนต์ และจักรยานยนต์ส่วนบุคคล

1.3 ข้อมูลที่จัดเก็บ

1.3.1 ข้อมูลที่จะจัดเก็บบนบัตรประจำตัวประชาชนแบบสมาร์ทการ์ด

ในการจัดทำบัตรประจำตัวประชาชนแบบสมาร์ทการ์ด จะมีการกำหนดพื้นที่บนบัตรและระบบการรักษาความปลอดภัยไว้ ทั้งนี้ความจุในชิพตามข้อกำหนดมีความจุ 66K แต่บัตรรุ่นแรกได้รับมีเพียง 28K ซึ่งตามแผนในเบื้องต้นได้มีการวางไว้ว่าจะมีการจัดเก็บประกอบด้วยข้อมูลที่สำคัญต่างๆ ได้แก่

1.3.1.1 ข้อมูลการทะเบียนราษฎร์ และทะเบียนอื่นๆ ที่จำเป็น

1.3.1.2 รูปภาพ

1.3.1.3 ลายพิมพ์นิ้วมือ (Finger Print) มีการจัดเก็บเป็นรหัสลายพิมพ์นิ้วมือ (MINUTAIE)

1.3.1.4 กุญแจเข้าสู่ระบบ (Public Key Infrastructure : PKI) เป็นกุญแจสาธารณะเข้าสู่ระบบ

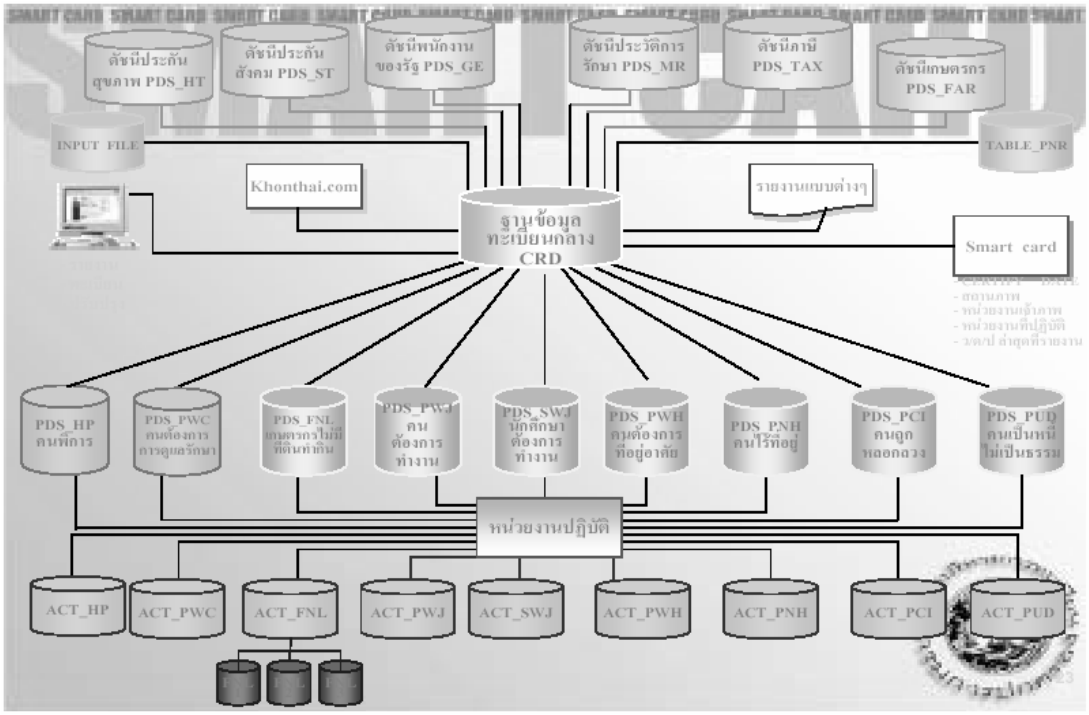
1.3.1.5 พื้นที่ของผู้ถือบัตรสำหรับเข้าใช้จดหมายอิเล็กทรอนิกส์ (Buffer E-Mail)

1.3.1.6 พื้นที่เก็บข้อมูลส่วนตัวของผู้ถือบัตร (Buffer e-Memo)

1.3.1.7 รหัสผ่านเข้าสู่ระบบของผู้ถือบัตร (User Password) และส่วนเชื่อมเครือข่าย (Authorization) เข้าสู่ระบบของแต่ละหน่วยงานที่เข้าเชื่อม (Application) ในแต่ละหน่วยงาน

ตามแผนการที่กรมการปกครองได้วางไว้ ข้อมูลที่จะให้บัตรสามารถจัดเก็บได้ และเข้าถึงในฐานข้อมูลของหน่วยงานที่จะเข้าร่วมในเบื้องต้นมี 4 หน่วยงานละ 1

โครงการ คือ กรมการปกครอง สำนักงานหลักประกันสุขภาพแห่งชาติ สำนักงานประกันสังคม สำนักงาน ก.พ. และโครงการจดทะเบียนคนจน โดยข้อมูลในแต่ละส่วนมีรายละเอียดดัง ภาพที่ 2



ภาพที่ 2 รูปแสดงฐานข้อมูลของหน่วยงานที่จะเข้าร่วม

ที่มา : สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์/ TU-RAC, การคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในบัตรประจำตัวแบบสมาร์ทการ์ด (Smart Card), (ม.ป.ท., 2547), 37

.

1.3.2 ข้อมูลที่จัดเก็บของสำนักทะเบียนกลาง กรมการปกครอง

ตารางที่ 1 ข้อมูลที่จัดเก็บในชิพบัตรประชาชนแบบสมาร์ทการ์ด ส่วนของสำนักงานทะเบียนกลาง

ลำดับ	รายการ	ชนิด	ขนาด	หมายเหตุ
1	เลขประจำตัวประชาชน	N	13	
2	ชื่อ-นามสกุล, คำนำหน้านาม	C	80	
3	ชื่อ-นามสกุล, คำนำหน้านาม (ภาษาอังกฤษ)	C	80	

ตารางที่ 1 (ต่อ)

ลำดับ	รายการ	ชนิด	ขนาด	หมายเหตุ
4	วันเดือนปี เกิด	N	8	DDMMYYYY
5	เพศ	N	1	1-ชาย, 2-หญิง
6	สัญชาติ	C	20	
7	ที่อยู่ปัจจุบัน	C	150	
8	ศาสนา	N	1	1.พุทธ,2.คริสต์,3.อิสลาม,4.ซิกข์,5.พราหมณ์-ฮินดู
9	เลขประจำตัวประชาชนของ บิดา	N	13	
10	ชื่อ-นามสกุล;คำนำหน้านามของ บิดา	C	80	
11	สัญชาติของ บิดา	C	20	
12	เลขประจำตัวประชาชนของ มารดา	N	13	
13	ชื่อ-นามสกุล;คำนำหน้านามของ มารดา	C	80	
14	สัญชาติของ มารดา	C	20	
15	วันเดือนปี ที่เปลี่ยนชื่อ –สกุลล่าสุด	N	8	DDMMYYYY
16	ชื่อ-นามสกุลเดิมก่อนเปลี่ยนล่าสุด	C	60	ชื่อ#นามสกุล
17	หมายเลข บัตร/คำร้อง	C	20	
18	สถานที่ / หน่วยงาน ที่ออกบัตร	C	100	
19	รหัสผู้ออกบัตร	C	10	
20	วันเดือนปี ที่ออกบัตร	N	8	DDMMYYYY
21	วันเดือนปี ที่บัตรหมดอายุ	N	8	DDMMYYYY
22	ภาพใบหน้า	B	5120	
23	เลขประจำประชาชน ของคู่สมรส	N	13	
24	ชื่อ-นามสกุลคู่สมรส	C	80	
25	วันเดือนปี ที่สมรส	N	8	DDMMYYYY
26	เลขที่ทะเบียนสมรส	C	15	
27	วันเดือนปี ที่หย่า	N	8	DDMMYYYY
28	เลขที่ทะเบียนหย่า	C	15	

ตารางที่ 1 (ต่อ)

ลำดับ	รายการ	ชนิด	ขนาด	หมายเหตุ
29	สถานที่เกิด	C	150	
30	บ้านที่แจ้งย้ายเข้าครั้งแรกหลังการเกิด	C	150	
31	วันเดือนปี ที่ย้ายเข้าบ้านครั้งแรกหลังการเกิด	N	8	DDMMYYYY
32	วันที่ปรับปรุงข้อมูล	DATE	8	DDMMYYYY

ที่มา : สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์/ TU-RAC, การคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในบัตรประจำตัวแบบสมาร์ทการ์ด (Smart Card), (ม.ป.ท., 2547), 38

1.3.3 ข้อมูลที่จะจัดเก็บของสำนักงานหลักประกันสุขภาพแห่งชาติ

ตารางที่ 2 ข้อมูลจัดเก็บในชิพบัตรประจำตัวประชาชนแบบสมาร์ทการ์ดส่วนของสำนักงานหลักประกันสุขภาพแห่งชาติ

ลำดับ	รายการ	ชนิด	ขนาด	รูปแบบ	หมายเหตุ
1	จังหวัดที่ขึ้นทะเบียนรักษา	C	30	สมุทรปราการ	
2	รหัสเครือข่ายสถานบริการ	C	10	1122330011	
3	สถานบริการหลัก/ร.พ. ส่งต่อ	C	5	11011	
4	สถานที่บริการรอง/หน่วยบริการปฐมภูมิ	C	5	12000	
5	วัน/เดือน/ปี พ.ศ.ที่เริ่มใช้สิทธิ	Date	8	12/04/47	
6	วัน/เดือน/ปี พ.ศ.ที่หมดอายุ	Date	8	12/04/52	
7	โรคประจำตัว	C	50x5=250	Hypertension	5 entries
8	รายการยาที่แพ้	C	50x5=250	Paracetamol	5 entries
9	หมู่โลหิต	C	3	A,B,AB	
10	การบริจาคอวัยวะ	C	3	Yes,No	

ตารางที่ 2 (ต่อ)

ลำดับ	รายการ	ชนิด	ขนาด	รูปแบบ	หมายเหตุ
11	ร.พ. ส่งต่อ	C	60	พระนั่งเกล้า	
12	วันที่ส่งต่อ	C	8		12/04/47
13	รหัสการจ่ายรายหัว	C	2	1,2	
14	จำนวนครั้งที่ย้ายสถานบริการ	C	6x12=72	2547_1	12 entries
15	จำนวนครั้งที่เข้ารับบริการฉุกเฉินใน ร.พ. หลัก	C	10x12=10	47_11011_1	12 entries
16	จำนวนครั้งที่เข้ารับการฉุกเฉินตามมาตรา 7	C	13x12=156	OP_47_19999_1	12 entries
17	วันที่ปรับปรุงข้อมูล	Date	8	ddmmyyyy	

ที่มา : สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์/ TU-RAC, การคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในบัตรประจำตัวแบบสมาร์ทการ์ด (Smart Card), (ม.ป.ท., 2547), 39

1.3.4 ข้อมูลที่จะจัดเก็บของสำนักงานประกันสังคม

ตารางที่ 3 ข้อมูลที่จัดเก็บในชิพบัตรประจำตัวประชาชนแบบสมาร์ทการ์ด ส่วนของสำนักงานประกันสังคม

ลำดับ	รายการ	ชนิด	ขนาด	รูปแบบ	หมายเหตุ
	สถานะและสิทธิ์				
1	สถานะผู้ประกันสังคม	C	1		
2	สิทธิประโยชน์ที่ได้รับ	C	7		
3	รหัสสถานพยาบาล	N	7		
4	ชื่อสถานพยาบาล	C	40		
5	วันที่ออกบัตรรับรองสิทธิ	DATE	8		
6	วันที่บัตรรับรองสิทธิหมดอายุ	DATE	8		

ตารางที่ 3 (ต่อ)

ลำดับ	รายการ	ชนิด	ขนาด	รูปแบบ	หมายเหตุ
	ประวัติการจ้าง				
7	เลขที่บัญชีนายจ้าง – 1	C	10		
8	สาขานายจ้าง - 1	C	6		
9	ชื่อนายจ้าง – 1	C	35		
10	สถานะว่าจ้าง – 1	C	1		
11	วันเข้างาน – 1	DATE	8	DDMMYYYY	
12	วันออกงาน – 1	DATE	8	DDMMYYYY	
13	วันที่ปรับปรุงข้อมูล	DATE	8	DDMMYYYY	

ที่มา : สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์/ TU-RAC, การคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในบัตรประจำตัวแบบสมาร์ทการ์ด (Smart Card), (ม.ป.ท., 2547), 40

หมายเหตุ PDS : Population Directory Subset หมายถึง ระบบฐานข้อมูลประชาชนกลุ่มย่อยตามประเภทต่าง ๆ เพื่อเชื่อมโยงและบรรจุข้อมูลลงในบัตรสมาร์ทการ์ด

1.3.5 ข้อมูลที่จะจัดเก็บของสำนักงาน ก.พ.

ตารางที่ 4 รายการข้อมูลข้าราชาการพลเรือนสามัญและลูกจ้างประจำ ที่จะจัดเก็บในชิพของบัตรประจำตัวประชาชนแบบสมาร์ทการ์ดสำหรับข้าราชการพลเรือนสามัญและลูกจ้างประจำ ของสำนักงาน ก.พ. (บัตรประจำตัวเจ้าหน้าที่ของรัฐ)

1. ข้อมูลข้าราชการพลเรือนสามัญ (Table : card_data)					
ลำดับ	**รายการ**	**ประเภท**	**ขนาด**	**คำอธิบาย**	**หมายเหตุ**
1	ENTRYCS	Text	8	วันบรรจุ	ววดดปปปป
2	MINDEPT	Text	5	รหัสส่วนราชการ	
3	ADMINPOST	Text	4	รหัสตำแหน่งทางบริหาร	
4	ADMINNAME	Text	50	ชื่อตำแหน่งทางบริหาร	
5	POSCODE	Text	6	รหัสตำแหน่งในสายงาน	
6	POSNAME	Text	50	ชื่อตำแหน่งในสายงาน	
7	LEVEL	Text	2	ระดับ	CODE LIST
8	XDEGREE	Text	1	รหัสระดับการศึกษาสูงสุด	CODE LIST
9	PROV	Text	2	รหัสจังหวัดที่ดำรงตำแหน่ง	CODE LIST
10	CNTRY	Text	3	รหัสประเทศที่ดำรงตำแหน่ง	CODE LIST
11	XTYPE	Text	2	รหัสประเภทข้าราชการ	1=พลเรือนสามัญ
12	XSUBTYPE	Text	2	รหัสสถานภาพเจ้าหน้าที่ของรัฐ	1= ข้าราชการ ,2= ลูกจ้างประจำ
13	STATUS	Text	1	สถานะการเป็นข้าราชการบำนาญ	0=ไม่เป็น,1=เป็น
14	ENTRDATE	Text	8	วันที่บันทึกข้อมูล	ววดดปปปป
15	EXPDATE	Text	8	วันที่ออกจากราชการ	ววดดปปปป
16	UPDATE	Date	8	วันที่ปรับปรุง	ววดดปปปป

ที่มา : สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์/ TU-RAC, การคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในบัตรประจำตัวแบบสมาร์ทการ์ด (Smart Card), (ม.ป.ท., 2547), 34

1.3.6 ข้อมูลที่จะจัดเก็บของโครงการจดทะเบียนคนจน

ตารางที่ 5 ข้อมูลที่จัดเก็บในชิพบัตรประจำตัวประชาชนแบบสมาร์ทการ์ด ส่วนของทะเบียนคนจน

ลำดับ	รายการ	ชนิด	ขนาด	หมายเหตุ
1	สถานที่ลงทะเบียน	C	40	
2	วันที่ลงทะเบียน	DATE	8	
3	ปัญหาที่ลงทะเบียน	C	8	แต่ละ Digit คือประเภทปัญหาที่ลงทะเบียน Digit 1 = สย.1, 2 = สย.2 , 3 = สย.3.....,8 = สย.8
4	สถานภาพการดำเนินการ	C	8	แต่ละ Digit คือสถานภาพการดำเนินการในแต่ละประเภทปัญหา Digit 1 เป็นสถานะของ สย.1, 2 = สย.2 , 3 = สย.3.....,8 = สย.8 ความหมายในแต่ละ Digit 1 = รอการแก้ไขปัญหา, 2 = ได้รับการแก้ไขแล้วแต่ยังไม่เสร็จสิ้น, 3 = ได้รับการแก้ปัญหาเสร็จสิ้นแล้ว
5	หน่วยงานที่ดำเนินการ	C	40	
6	การให้ความช่วยเหลือ	C	100	
7	วันที่ปรับปรุงข้อมูล	DATE	8	DDMMYYYY

ที่มา : สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์/ TU-RAC, การคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในบัตรประจำตัวแบบสมาร์ทการ์ด (Smart Card), (ม.ป.ท., 2547), 42

ทั้งนี้ในท้ายสุดจากปัญหาความไม่พร้อมของความจุในหน่วยความจำของชิพ ทำให้กรมการปกครองในฐานะหน่วยงานกลางที่ดูแลระบบบัตรประจำตัวประชาชนแบบสมาร์ทการ์ดนี้ ได้ดำเนินการจัดเก็บเฉพาะในส่วนของข้อมูลทะเบียนราษฎร์และบัตรประจำตัวประชาชนเดิม โดยข้อมูลของหน่วยงานอื่นคือ สำนักงานหลักประกันสุขภาพแห่งชาติ สำนักงานประกันสังคม สำนักงาน ก.พ. และโครงการจดทะเบียนคนจน ได้ชะลอไว้ก่อนจนกว่าจะแก้ไขปัญหาระบบเทคโนโลยีได้ และได้ข้อยุติในส่วนบัตรประจำตัวเจ้าหน้าที่ของรัฐที่มีกฎหมายบังคับใช้อยู่แล้วว่าจะต้องยกเลิกหรือแก้ไขเพิ่มเติมอย่างไรให้สอดคล้องกับการดำเนินการรวมบัตรเจ้าหน้าที่ของรัฐไว้ในบัตรประจำตัวประชาชนเพียงใบเดียว

1.4 ระบบการใช้งาน (สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการสถาบันวิจัยและให้คำปรึกษาแห่ง มหาวิทยาลัยธรรมศาสตร์/ TU-RAC 2547 : 23 - 47)

1.4.1 ระบบการใช้งานกับบัตรประจำตัวประชาชนแบบสมาร์ทการ์ด

บัตรประจำตัวประชาชนแบบสมาร์ทการ์ดที่นำมาใช้ในประเทศไทยนั้น ได้มีการวางระบบให้มีความสามารถในการใช้งานที่หลากหลาย

1.4.1.1 ใช้ตามวัตถุประสงค์ของบัตรประจำตัวประชาชนและทะเบียนบ้าน

1.4.1.2 ใช้เป็น Master Key ในการเข้าสู่ระบบบริการ (e-Service) แบบ On-line

1.4.1.3 ใช้งานแบบ Off-line เพื่อเก็บสำเนารายการทะเบียนต่าง ๆ และเพื่อบริการประชาชนในระบบเปลี่ยนผ่านไปสู่ระบบ On-line

1.4.1.4 ใช้เป็นบัตร PKI

1.4.1.5 ใช้เป็นบัตรเงินสด

1.4.1.6 ใช้เป็นหนังสือเดินทาง

1.4.1.7 ใช้เป็นใบขับขี่

1.4.1.8 ใช้เป็นบัตร Security Access

1.4.2 ระบบการคุ้มครองข่าวสารส่วนบุคคลที่วางไว้สำหรับบัตรแบบสมาร์ทการ์ด

พัฒนาการของเทคโนโลยีต่าง ๆ ในโลกปัจจุบัน โดยเฉพาะอินเทอร์เน็ต ทำให้โลกทั้งโลกสามารถเข้าถึงข้อมูลต่าง ๆ ในโลกได้ จึงส่งผลให้ข้อมูลข่าวสารกลายเป็นเรื่องสำคัญ จนมีผู้กล่าวว่าบุคคลใดครอบครองข้อมูลข่าวสารมากที่สุด บุคคลนั้นจะครอบครองโลก ซึ่งรวมทั้งข้อมูลข่าวสารส่วนบุคคลที่เป็นที่ต้องการของบุคคลบางกลุ่ม ไม่ว่าจะในด้านธุรกิจ ด้านความมั่นคงแห่งชาติหรือการนำข้อมูลข่าวสารส่วนบุคคลมาก ซึ่งหากบุคคลใดได้ข้อมูลดังกล่าวไป อาจส่งผลด้านลบแก่เจ้าของข้อมูลข่าวสารส่วนบุคคลนั้นได้

ปัญหาความปลอดภัยของข้อมูลบนบัตรประชาชนแบบสมาร์ทการ์ดจึงเป็นประเด็นหลักที่นักกฎหมายและนักวิชาการต่างหยิบยกขึ้นมาเป็นประเด็นในการแสดงความคิดเห็นต่อบัตรประชาชนแบบสมาร์ทการ์ด ซึ่งความปลอดภัยจะต้องเริ่มต้นจากการสร้างชิพคอมพิวเตอร์โดยโรงงานผู้ผลิตที่มีการออกแบบโครงสร้างและการทำงานที่ถูกต้องและสามารถป้องกันการลักลอบดักข้อมูลที่สำคัญจากตัวชิพได้ มิเช่นนั้นอาจมีการขโมยความลับของข้อมูลต่างๆ ได้โดยง่าย นอกจากชิพคอมพิวเตอร์แล้ว โปรแกรมที่ใช้ควบคุมการทำงานของบัตร (Card Operating system) จะต้องได้รับการออกแบบที่ดีด้วย เนื่องจากมีความเป็นไปได้ที่จะมีการทุจริตโดยผู้ออกแบบและผู้สร้างตัวโปรแกรมนี้ อาจใส่โปรแกรมบางอย่างลงไป เรียกว่า Trap Door เพื่อที่จะอำนวยความสะดวกในการขโมยหรือเปลี่ยนแปลงข้อมูลที่สำคัญบนบัตร โดยไม่ได้ตรวจสอบหรือมีการรับรองทางอิเล็กทรอนิกส์อย่างถูกต้อง วิธีการโกงนี้ยากแก่การตรวจสอบ ดังนั้นการเลือกใช้ระบบสมาร์ทการ์ดจะต้องเลือกระบบที่น่าเชื่อถือ และได้รับการพิสูจน์การใช้งานแล้วในวงกว้าง

การใช้บัตรโดยไม่ได้รับอนุญาต ก็เป็นอีกปัญหาหนึ่งเนื่องจากในระบบสมาร์ทการ์ดมีการใช้หมายเลข PIN เพียงผู้เดียว ในการแสดงตัวว่าเป็นผู้ได้รับอนุญาตอย่างถูกต้องจะมีผู้รู้หมายเลข PIN เพียงผู้เดียว คือ ผู้เป็นเจ้าของบัตร แต่อย่างไรก็ตาม อาจมีความเสี่ยงต่อการทุจริตได้จากการรั่วไหลของหมายเลข PIN จึงมาเทคโนโลยีมาแก้ไขปัญหานี้ คือเทคโนโลยีไบโอเมทริก (Biometric Identification) ซึ่งระบบนี้จะสามารถบอกได้ว่าผู้ใช้บัตรได้รับอนุญาตอย่างถูกต้องหรือไม่ โดยการตรวจสอบส่วนใดส่วนหนึ่งของร่างกาย เช่น ลายนิ้วมือ เยื่อภายในลูกตา หรือเสียงพูด เป็นต้น

สำหรับในการนี้ประเทศไทยได้มีระบบการคุ้มครองข้อมูลข่าวสารส่วนบุคคลที่วางไว้สำหรับบัตรอเนกประสงค์ได้มีการดำเนินงานตั้งแต่การวางระบบความปลอดภัยและป้องกันการปลอมแปลงในการจัดทำบัตรใน 7 ประการ คือ

1. วัสดุตัวบัตร
2. ข้อมูลที่ใช้ในการจัดทำบัตร
3. การพิมพ์และการเคลือบบัตร (วัสดุบัตร)
4. กุญแจที่ใช้เชื่อมข้อมูล (Media) ที่อยู่บนวัสดุตัวบัตร
5. การตรวจสอบและพิสูจน์วัสดุตัวบัตรและวัสดุบัตร
6. การควบคุมการผลิต การเก็บรักษา และการเบิกจ่ายวัสดุตัวบัตรและวัสดุบัตร
7. การกำหนดขั้นตอนการออกบัตรที่รัดกุม

ทั้งนี้ระบบกลไกการควบคุมและรักษาความปลอดภัยข้อมูลที่บรรจุภายในบัตรประจำตัวประชาชนแบบสมาร์ทการ์ด ทางกรมการปกครองได้มีการวางระบบไว้ซึ่งเป็นมาตรฐานของเทคโนโลยีที่ใช้ในต่างประเทศที่พิจารณาจาก 2 มิติ ได้แก่

1.4.3 บุคคลที่มีความสามารถในการเข้าถึงข้อมูลในบัตร

ประเด็นของบุคคลที่มีความสามารถในการเข้าถึงข้อมูล นับเป็นเรื่องสำคัญอันดับแรก ซึ่งการเข้าถึงข้อมูลในบัตรนั้นอาจแบ่งได้เป็น 3 กลุ่ม คือ

1.4.3.1 ทุกคน โดยบัตรประจำตัวแบบอเนกประสงค์บางแบบไม่จำเป็นต้องใช้รหัสผ่าน (Password) ใครก็ตามที่ถือบัตรดังกล่าว สามารถเข้าถึงข้อมูลได้ เช่น บัตรคนไข้ (Medical card) ที่มีชื่อคนไข้และกลุ่มเลือด ซึ่งสามารถอ่านได้โดยไม่ต้องใช้รหัสผ่าน

1.4.3.2 เฉพาะผู้ถือบัตร โดยรูปแบบของรหัสผ่านส่วนมากที่ผู้ถือบัตรมีไว้เรียกว่ารหัสประจำตัว หรือ PIN ซึ่งเป็นเลข 4 หรือ 5 หลัก โดยพิมพ์อยู่บนแป้นกด (Key pad) เพราะฉะนั้นหากมีบุคคลที่ไม่ได้รับอนุญาตพยายามใช้บัตร มันจะมีการล็อคภายหลังจากที่พยายามกดหรือใส่รหัสประจำตัวไม่สำเร็จ 3 ครั้ง ทั้งนี้ปัจจุบันรหัสผ่านมีการพัฒนารูปแบบที่ทันสมัยมากขึ้น

1.4.3.3 เฉพาะบุคคลที่สาม โดยบัตรประจำตัวแบบสมาร์ทการ์ดบางแบบอนุญาตให้เฉพาะบุคคลที่ระบุไว้เท่านั้นที่ใช้มันได้ เช่น บัตรเบิกเงินสด หรือ Electronic Purse ที่ธนาคารเจ้าของบัตรเท่านั้นสามารถทำการโหลดข้อมูลใหม่ได้

1.4.4 ความสามารถที่จะเข้าถึงข้อมูล

เนื่องจากความสามารถของชิพที่บรรจุข้อมูลได้มากกว่าบัตรแถบแม่เหล็ก ดังนั้นข้อมูลที่อยู่บนบัตรประจำตัวแบบสมาร์ทการ์ดนั้นจึงแบ่งออกเป็นหลายส่วน เพื่อป้องกันมิให้ข้อมูลทั้งหมดถูกล่วงละเมิดโดยง่าย ซึ่งอาจแบ่งข้อมูลที่จะจัดเก็บบนบัตรเป็น 4 ประการ

1. ข้อมูลที่ปรับปรุงได้เพียงอย่างเดียว
2. ข้อมูลที่เพิ่มได้อย่างเดียว
3. ข้อมูลที่ปรับปรุงหรือเปลี่ยนแปลงได้อย่างเดียว
4. ข้อมูลที่ไม่สามารถเข้าไปทำอะไรได้เลย

โดยปกติสมาร์ทการ์ดสามารถจำกัดการใช้ข้อมูลกับบุคคลที่ได้รับอนุญาต 1 คน ด้วยรหัสผ่าน 1 ชุด อย่างไรก็ดี หากมีการส่งข้อมูลด้วยวิทยุหรือโทรศัพท์แล้ว จำเป็นต้องมีการป้องกันเพิ่มเติม โดยรูปแบบหนึ่งของการป้องกันคือ การแปลงรหัส (Ciphering) ซึ่งเป็นเสมือนการแปลข้อมูลให้เป็นภาษาที่ไม่รู้เรื่อง บัตรบางแบบสามารถทำได้ทั้งการแปลงรหัสและการถอดรหัส (Deciphering) ซึ่งเป็นการแปลงกลับมาให้อยู่ในรูปแบบที่เข้าใจได้ง่ายขึ้น ดังนั้นจึงสามารถส่งข้อมูลออกไปได้โดยไม่ต้องห่วงเรื่องความลับจะถูกเปิดเผย

ปัญหาของการกระทบต่อสิทธิเสรีภาพโดยเฉพาะข้อมูลส่วนบุคคลในบัตรประจำตัวประชาชนแบบสมาร์ทการ์ดนี้ทางกรมการปกครองได้ยืนยันว่าจะไม่ลิดรอน แต่กลับเป็นการส่งเสริมและคุ้มครองสิทธิส่วนบุคคลมากกว่า เพราะมีบัตรเดียวก็สามารถเข้าใช้บริการขั้นพื้นฐานของหน่วยงานของรัฐได้ทุกหน่วยงาน เมื่อขอมีบัตรประจำตัวประชาชนแบบสมาร์ทการ์ด สามารถทำได้รวดเร็ว ติดต่อเพียงสำนักทะเบียนแห่งเดียวและเมื่อบัตรประจำตัวประชาชนแบบสมาร์ทการ์ดสูญหายไม่ต้องกังวล เนื่องจากประการแรกการเปิดดูข้อมูลบนบัตร จะต้องให้เจ้าของบัตรอนุญาต โดยพิมพ์ลายนิ้วมือและเจ้าหน้าที่ที่เกี่ยวข้องตามกฎหมายจึงจะเข้าดูได้ ประกอบกับข้อมูลบนบัตรเป็นเพียงข้อมูลทั่วไปประมาณ 10% ของข้อมูลทั้งหมด ส่วนอีก 90% ที่เป็นข้อมูลลึก ๆ จะอยู่ที่หน่วยเก็บข้อมูลของหน่วยงานที่ประชาชนไปติดต่อ บัตรประจำตัวประชาชนแบบสมาร์ทการ์ดเป็นเพียงกุญแจเปิดไปยังข้อมูลดังกล่าว ดังนั้นบัตรปลอมหรือหากบัตรหายผู้ปลอมหรือผู้เก็บบัตรได้ก็ไม่สามารถเปิดดูข้อมูลของเจ้าของบัตร และนำไปใช้ในทางที่ไม่ถูกต้องได้

2. เว็บเซอร์วิส (Web Services) (วิศิษฎ์ นวอิทธิพร, สมพล แซ่ปึง และสิริวรรณ พรกิตติวัฒนากุล 2547 : 10-17)

2.1 ความหมายของเว็บเซอร์วิส

เว็บเซอร์วิส (Web Services) คือ แอพพลิเคชันหรือโปรแกรม ซึ่งทำงานอย่างใดอย่างหนึ่งในลักษณะให้บริการ โดยจะถูกเรียกใช้งานจาก แอพพลิเคชัน หรือ โปรแกรมอื่นๆ ผ่านเว็บ ในรูปแบบ RPC (Remote Procedure Call) หรือระบบสั่งงานระยะไกล การให้บริการของเว็บเซอร์วิส จะมีเอกสารอธิบายคุณสมบัติของบริการกำกับไว้มีภาษาที่ถูกใช้เป็นสื่อในการแลกเปลี่ยนข้อมูล คือ XML (Extensible Markup Language) ทำให้ผู้ใช้สามารถเรียกใช้บริการต่างๆของ แอพพลิเคชัน ที่อยู่บนแพลตฟอร์ม ใด ๆ ก็ได้ บนโพรโตคอล HTTP สำหรับ World Wide Web อันเป็นช่องทางที่ได้รับการยอมรับทั่วโลก ในการติดต่อสื่อสาร กันระหว่าง แอพพลิเคชัน กับ แอพพลิเคชัน และมีการนำเสนอให้สาธารณชนรับทราบ ผู้ใช้บริการจึงสามารถค้นหาเว็บเซอร์วิส ได้โดยที่ไม่จำเป็นต้องรู้ที่อยู่จริงของแอปพลิเคชัน หรือโปรแกรมนั้น

2.2 มาตรฐานที่ใช้ในการพัฒนาเว็บเซอร์วิส

มาตรฐานในการพัฒนาเว็บเซอร์วิส ที่สำคัญมี 3 อย่าง ดังนี้

2.2.1 SOAP (Simple Object Access Protocol)

เป็น XML-based โปรโตคอล (Protocol) สำหรับ การแลกเปลี่ยนข้อมูลในสภาวะแวดล้อมแบบกระจายศูนย์ (decentralized, distributed environment) SOAP ได้ กำหนด

เมเสจจิ้งโปรโตคอล (Messaging Protocol) ระหว่างผู้ขอบริการ (requestor) กับผู้ให้บริการ (provider) เช่น ผู้ขอบริการสามารถติดต่อแลกเปลี่ยนข้อมูลกับผู้ให้บริการโดยใช้ RMI (Remote Method Invocation) ตามวิธีการของ โปรแกรมเชิงวัตถุ บริษัทไมโครซอฟท์ ไอบีเอ็ม โลตัส ยูสเซอร์แลนด์ (User Land) และ ดีเวลลอปเปอร์เมนเตอร์ (Developer Mentor) ได้ร่วมกันกำหนดมาตรฐานของ SOAP ขึ้น ซึ่งต่อมาได้มีบริษัทอีก 30 กว่าบริษัทเข้าร่วม และจัดตั้งเป็น W3C XML Protocol Workgroup ขึ้น SOAP ได้กำหนดรูปแบบพื้นฐานของการสื่อสารแบบกระจายขึ้นโดย การพัฒนา SOA แม้ว่า SOA จะไม่ได้กำหนดเมจเสจจิ้งโปรโตคอลไว้ แต่ SOAP ได้ถูกกำหนดให้เป็น Services-Oriented Architecture Protocol เรียบร้อยแล้ว เนื่องจากได้ถูกใช้ในการพัฒนา SOA อย่างแพร่หลายแล้วนั่นเอง จุดเด่นของ SOAP ก็คือเป็นโปรโตคอลที่เป็นกลาง กล่าวคือ ไม่มีใครเป็นเจ้าของ และเป็นโปรโตคอล ที่ทำงานกับโปรโตคอลอื่นหลายชนิดการพัฒนาก็อนุญาตให้ทำได้อย่างอิสระตามแพลตฟอร์มระบบปฏิบัติการ แบบจำลองทางวัตถุ (Object model) และภาษาโปรแกรมของผู้ที่ทำการพัฒนา

ดังนั้น SOAP เป็นโปรโตคอลชนิดหนึ่งที่ทำให้เว็บเซิร์ฟเวอร์สามารถติดต่อและเข้าใจเว็บเซอร์วิสได้ (ไม่สนใจว่าอยู่บน Platform ใด) และ SOAP ทำงานอยู่บนโปรโตคอล HTTP ซึ่งเป็นโปรโตคอลมาตรฐาน ดังนั้น SOAP จึงทำงานผ่าน Firewall ได้โดยไม่ติดปัญหาแต่อย่างใด

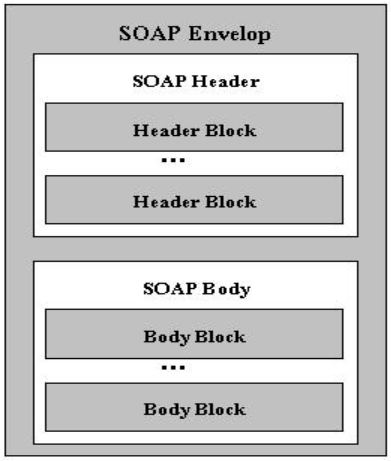
2.2.1.1 โครงสร้างของ SOAP

เอกสาร SOAP นั้นมีโครงสร้างในรูปแบบ XMLซึ่งเราสามารถแบ่งเป็นส่วนของเอกสารได้เป็น 3 ส่วนหลัก ตามภาพที่ 3 ดังนี้คือ

2.2.1.1.1 SOAP Envelope เป็นส่วนเนื้อหาสาระของเอกสารทั้งหมดเป็นส่วนนอกสุดห่อหุ้มข่าวสารทั้งหมดเอาไว้

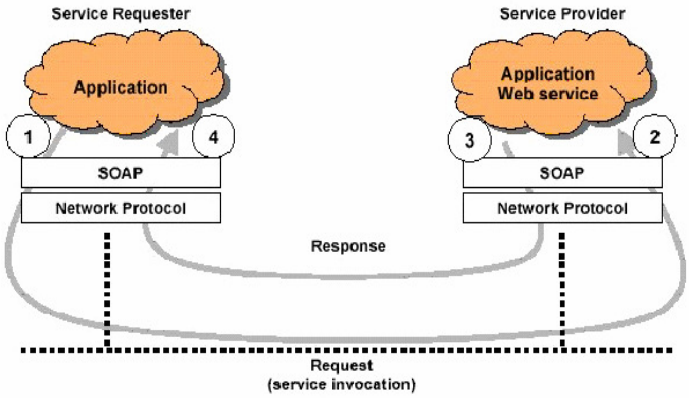
2.2.1.1.2 SOAP Header เป็นที่บรรจุเอาคุณลักษณะและค่าที่แสดงถึงวิธีการติดต่อเรียกใช้บริการ

2.2.1.1.3 SOAP Body เป็นพื้นที่เก็บข้อมูลสำหรับรับข่าวสารและวิธีการตอบข้อผิดพลาดกลับไป



ภาพที่ 3 โครงสร้างของเอกสาร SOAP

ที่มา : HPCC Wiki, เอกสารเรื่องเว็บเซอร์วิสคืออะไร [ออนไลน์], เข้าถึงเมื่อ 20 ธันวาคม 2549. ได้จาก http://mike.cpe.ku.ac.th/~ekkasit/files/tutorials/SOA-www.hpcc.nectec.or.th.doc



ภาพที่ 4 แสดงลักษณะข้อความที่รับ - ส่ง ผ่านโพรโตคอล SOAP ซึ่งเป็นไปตามรูปแบบของ XML

ที่มา : HPCC Wiki, เอกสารเรื่องเว็บเซอร์วิสคืออะไร [ออนไลน์], เข้าถึงเมื่อ 20 ธันวาคม 2549. ได้จาก http://mike.cpe.ku.ac.th/~ekkasit/files/tutorials/SOA-www.hpcc.nectec.or.th.doc

จากภาพที่ 4 อธิบายได้ดังนี้

ผู้ขอใช้บริการ (Service Requester) สร้าง SOAP Message เพื่อเรียกใช้บริการของเว็บเซอร์วิส แล้วส่งผ่านโปรโตคอลเครือข่ายไปยังผู้ให้บริการ ในที่นี้ SOAP message ที่รับ-ส่งไปมานั้น อยู่ในรูปแบบ XML และต้องมีการแปลงกลับมาอยู่ในรูปแบบที่โปรแกรมหรือเว็บเซิร์ฟเวอร์เข้าใจ โดยมีโปรแกรมที่ทำหน้าที่แปลความหมายของเอกสาร XML คือ XML Parser

ผู้ให้บริการ (Service Provider) ได้รับ SOAP Message จากผู้ขอใช้บริการ จากนั้น จึงแปลข้อความนั้นกลับมาอยู่ในรูปแบบที่เว็บเซิร์ฟเวอร์เข้าใจ แล้วตรวจสอบว่าผู้ใช้บริการต้องการเรียกใช้เว็บเซอร์วิส ชื่ออะไร วิชาการอะไร และส่งพารามิเตอร์อะไร มาด้วย จากนั้นจึงส่งไปให้แก่คอมโพเนนต์ที่ให้บริการเว็บเซอร์วิส นั้นๆดำเนินการประมวลผล

หลังจากคอมโพเนนต์ที่ให้บริการเว็บเซอร์วิสส่งผลลัพธ์กลับมาแล้ว ผู้ให้บริการก็จะสร้าง SOAP Message ที่มีผลลัพธ์นั้นออกมาด้วย แล้วจึงส่งผ่านทางโปรโตคอลเครือข่ายกลับคืนไปยังผู้ขอใช้บริการ

ผู้ขอใช้บริการได้รับ SOAP Message ที่อยู่ในรูปแบบ XML จึงแปลข้อความนั้นกลับมาในรูปแบบที่โปรแกรมของผู้ขอใช้บริการเข้าใจ แล้วนำผลลัพธ์ไปใช้งาน เช่น แสดงผล หรือไปทำอย่างอื่น แล้วแต่ว่ามีการเขียนโปรแกรมรองรับไว้ให้ทำอย่างไรและจะมี SOAP Listener ทำหน้าที่คอยรับฟังว่ามีการเรียกใช้เว็บเซอร์วิสจากผู้ใช้ การบริการของเว็บเซอร์วิส แต่ละบริการจะมีไฟล์ SOAP Listener จำนวน 1 ไฟล์ เมื่อใดที่มีการเรียกใช้เว็บเซอร์วิส ไฟล์โปรแกรมที่เป็น SOAP Listener ก็จะไปปลุกให้เว็บเซอร์วิสทำงาน

2.2.1.2 ข้อดีของการใช้โพรโตคอล SOAP (Protocol SOAP)

2.2.1.2.1 โพรโตคอล SOAP สามารถให้เราเรียกใช้คอมโพเนนต์หรือ เว็บเซอร์วิส ข้ามเครื่อง ข้ามแพลตฟอร์มหรือข้ามภาษา ได้โดยอาศัยโพรโตคอลที่มีอยู่เดิมในอินเทอร์เน็ต อย่าง HTTP

2.2.1.2.2 โครงสร้างข้อมูลของ SOAP เป็นรูปแบบข้อความที่สื่อสารกันด้วยภาษา XML ซึ่งมีลักษณะเป็นข้อความธรรมดาๆปิดล้อมด้วยแท็ก (Tag) ทำให้เข้าใจได้ในทุกแพลตฟอร์ม

2.2.1.2.3 โพรโตคอล SOAP สามารถทำงานผ่านระบบไฟล์วอลล์ได้ง่าย เนื่องจาก SOAP ทำงานอยู่กับโพรโตคอล HTTP ซึ่งโดยธรรมชาติของไฟล์วอลล์ จะเปิดให้การสื่อสารด้วย HTTP ผ่านได้อย่างสะดวก

2.2.1.2.4 SOAP นั้นสนับสนุนจากหลายค่าย เช่น IBM, MS, SUN

2.2.1.3 ข้อเสียของการใช้โพรโตคอล SOAP

2.2.1.3.1 เนื่องจากลักษณะของ SOAP message เป็นเอกสาร XML ทำให้เสียเวลาในการแปลกลับมาเป็นรูปแบบที่โปรแกรมเข้าใจ

2.2.1.3.2 ในกรณีที่ SOAP ทำงานอยู่กับโพรโตคอล HTTP ซึ่งมีสมรรถนะในการรับ-ส่งข้อมูลต่ำกว่าโพรโตคอล DCOM, RMI, หรือ IIOP จึงทำให้โพรโตคอล SOAP มีอัตราการรับ-ส่งข้อมูลต่ำ

2.2.2 WSDL (Web Services Description Language)

เป็นภาษาที่ใช้อธิบายคุณลักษณะการใช้บริการของเว็บเซอร์วิส และวิธีการติดต่อกับเว็บเซอร์วิส โดยใช้ภาษา XML, WSDL เกิดจากการรวมแนวคิดของ NASSL (Network Accessible Service Specification Language), WDS (Well-Defined Services) ของบริษัทไอบีเอ็ม, SDL (The Service Description Language) และ SCL (the SOAP Contract Language) ของบริษัทไมโครซอฟท์ ปัจจุบัน WSDL เป็นภาษาที่อยู่ในการดูแลของ W3C (World Wide Web Consortium) ซึ่งยังไม่เป็นมาตรฐานที่สมบูรณ์ เวอร์ชั่นที่ใช้งานอยู่ในปัจจุบันคือ WSDL 1.1

ดังนั้น WSDL จึงเป็น โปรโตคอล ที่มีหน้าที่เสมือนคู่มือคำอธิบาย โดย WSDL จะอยู่ในรูปภาษา XML ที่อธิบายส่วนประกอบต่างๆ ของเว็บเซอร์วิส ไม่ว่าจะเป็นชื่อของ Method, Parameters, Data, Data types, Result, Return etc.

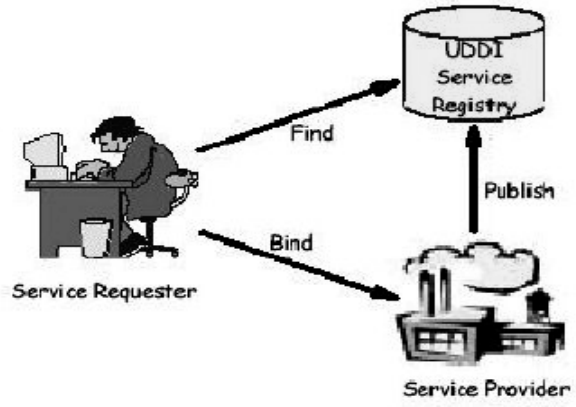
2.2.3 UDDI (Universal Description, Discovery, and Integration)

UDDI เป็นมาตรฐานที่ให้ชุดพื้นฐาน APIs (Application Programming Interface) ของ SOAP ที่สามารถนำมาใช้ในการพัฒนาเป็นตัวแทนของผู้ให้บริการ (Service broker) UDDI ใช้สำหรับค้นหาบริการที่ต้องการ และเมื่อได้มาแล้ว UDDI ยังจัดหาข้อตกลงในวิธีการที่จะใช้งานเปรียบได้กับบริการ Search Engine รูปแบบหนึ่ง

UDDI เป็นมาตรฐานที่จัดตั้งขึ้นโดยบริษัทไอบีเอ็ม บริษัทไมโครซอฟต์ และบริษัทอารีบา (Ariba) ปัจจุบันมีบริษัทที่ร่วมกันกำหนดมาตรฐานของ UDDI มากกว่า 70 บริษัท ซึ่งมาตรฐานของ UDDI ถูกกำหนดให้เป็นมาตรฐานสำหรับ B2B interoperability ในการทำธุรกิจอย่างใดไม่ก็อย่างหนึ่ง

UDDI เป็นที่ที่เตรียมกลไกสำหรับลงทะเบียนแบ่งหมวดหมู่ของเว็บเซอร์วิสที่จะนำเสนอไว้ และเป็นที่ที่สามารถค้นหาเว็บเซอร์วิสที่ต้องการได้ด้วยตัวของ UDDI เองก็เป็นเว็บเซอร์วิส ผู้ใช้งานสามารถติดต่อกับ UDDI ได้ด้วยข่าวสาร SOAP เมื่อมีการค้นหาเว็บเซอร์วิส ในส่วนของผู้พัฒนาจะมีการสอบถามบริการเว็บเซอร์วิสและค้นหาธุรกิจที่มีรูปแบบของการบริการที่ต้องการ ผู้พัฒนาจะได้รับไฟล์ดับเบิ้ลยูเอสดีแอล (WSDL) ซึ่งอธิบายถึงอินเทอร์เฟซของบริการเหล่านั้น UDDI นั้นเป็นรีจีสทรีชนิดที่มีวัตถุประสงค์ทั่ว ๆ ไป ที่สามารถใช้ลงทะเบียนบริการโปรแกรมใดๆ ก็ได้ไม่จำกัดเพียงแค่เว็บเซอร์วิสอย่างเดียวเท่านั้น UDDI ไอไม่ได้จำกัดว่าบริการที่จะลงทะเบียนนั้น ต้องสนับสนุนอินเทอร์เฟซของ SOAP หรือว่าจะต้องอธิบายโดยใช้ WSDL (Web

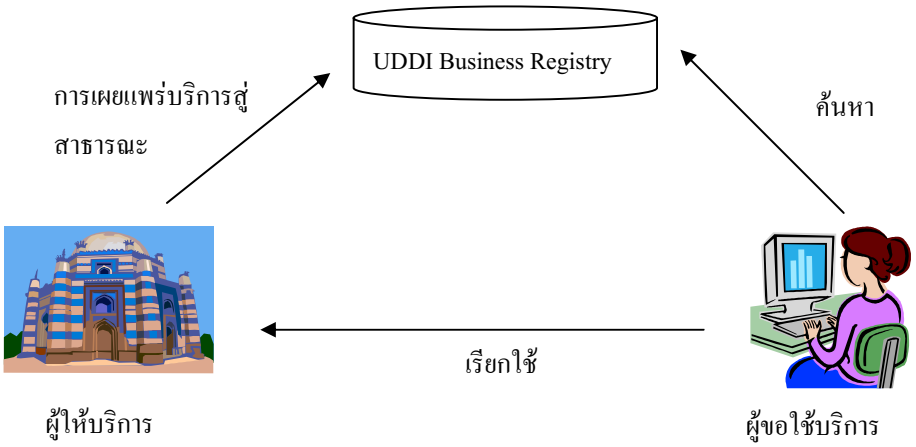
Service Description Language) ซึ่งในการใช้เทคโนโลยีของเว็บเซอร์วิส เหล่านี้ไม่ได้มีข้อจำกัดใดๆ แต่การที่ใช้เทคโนโลยีเหล่านี้ร่วมกันนั้น จะเป็นการเพิ่มประสิทธิภาพในการทำงานให้ดียิ่งขึ้น



ภาพที่ 5 ความสัมพันธ์ระหว่าง Requester กับ Provider และ UDDI
ที่มา : สราวุธ อ้อยศรีสกุล, ถอดรหัส .net + Web Services (กรุงเทพฯ : วิตตี้ กรุ๊ป, 2544), 127.

จากภาพที่ 5 UDDI เปรียบเสมือนฐานข้อมูลที่เก็บรายละเอียดของเว็บเซอร์วิสไว้ และรอให้ผู้ใช้บริการมาค้นหาบริการ บทบาทนี้เรียกว่า Service Discovery ส่วนในกรณีของผู้ให้บริการก็ต้องนำข้อมูลเกี่ยวกับ เว็บเซอร์วิสของตนไปเก็บไว้ใน UDDI บทบาทนี้ของ UDDI คือ การเผยแพร่บริการสู่สาธารณะ (Service Publication)

2.3 หลักการทำงานของเว็บเซอร์วิส



ภาพที่ 6 แสดงความสัมพันธ์ของผู้ใช้บริการกับผู้ให้บริการ และ UDDI
ที่มา : สราวุธ อ้อยศรีสกุล, ถอดรหัส .net + Web Services (กรุงเทพฯ : วิตตี้ กรุ๊ป, 2544), 231.

จากภาพที่ 6 สามารถอธิบายความสัมพันธ์ของผู้ใช้บริการกับผู้ให้บริการ และ UDDI ดังต่อไปนี้

2.3.1 ผู้ให้บริการเว็บเซอร์วิส เป็นผู้สร้างเว็บเซอร์วิสให้สามารถนำไปใช้ได้ในระบบอินเทอร์เน็ต และสร้างไฟล์เพื่ออธิบายการใช้เว็บเซอร์วิส และนำไปประกาศสู่สาธารณะ โดยมีการบอกถึงแหล่งที่ให้บริการเว็บเซอร์วิสและที่อยู่ของไฟล์ รวมทั้งชี้ถึงตำแหน่งที่เก็บไฟล์ที่ใช้ในการอธิบายใช้

2.3.2 ผู้ขอเรียกใช้บริการ (Service Client) จะค้นหาบริการเว็บเซอร์วิสที่เปิดให้ใช้บริการจากทะเบียนเว็บเซอร์วิส แล้วทำการดึงข้อมูลที่อธิบายการใช้งานของเว็บเซอร์วิสมาใช้ติดต่อกับผู้ให้บริการเพื่อเรียกใช้บริการ และแลกเปลี่ยนข้อมูลกับผู้ให้บริการ

2.3.3 ทะเบียนของเว็บเซอร์วิส (UDDI Registry) นั้นเป็นเสมือนศูนย์กลางของเว็บเซอร์วิส เพราะว่าเป็นตัวกลางที่คอยเก็บคำอธิบายสำหรับเว็บเซอร์วิส รวมทั้งชี้ถึงตำแหน่งที่เก็บไฟล์ที่ใช้ในการอธิบายการใช้งานของเว็บเซอร์วิสและให้รายชื่อของบริการประเภทต่างๆและแต่ละประเภทมีรายชื่อของผู้ให้บริการเว็บเซอร์วิส มีการสร้างขึ้นที่สร้างโดย ผู้ให้บริการเว็บเซอร์วิส

2.4 XML (The Extensible Markup Language) (ฐานันดร์ พงศ์ภัทรวัฒน และ ประภัทร์ รุ่งเรืองอนันต์ 2547 : 23-31)

2.4.1 ความหมายของ XML (The Extensible Markup Language) เป็นภาษาที่ได้รับการออกแบบมาเพื่อให้สามารถนิยามความหมายของข้อมูลได้ หรือที่เรียกว่า Data Definition โดยอนุญาตให้ผู้ใช้งานสร้างแท็กขึ้นเองได้ และแท็กที่สร้างขึ้นเองนั้นก็จะเป็นมาตรฐานที่ผู้ใช้กำหนดขึ้น และภาษาอื่นก็สามารถเรียกใช้ได้ ไม่ว่าจะเป็น VB, ASP, ASP.NET, PHP, JavaScript เพราะว่าแท็กที่ผู้ใช้สร้างขึ้นเองนั้นไม่ได้ทำหน้าที่แสดงข้อมูล แต่ทำหน้าที่ระบุขอบเขตของข้อมูล สำหรับผู้ที่ทำหน้าที่รับผิดชอบ และกำหนดมาตรฐานของ XML คือ World Wide Web Consortium (W3C)

ความแตกต่างระหว่าง XML กับ HTML คือ HTML ถูกนำมาใช้ในการสร้างเว็บเพจ ที่สามารถแสดงผลได้โดยโปรแกรมบราวเซอร์ แต่ XML จะใส่แท็กได้อย่างอิสระ แล้วทำการส่ง XML ชุดนี้ไป ประมวลผลยังแอพพลิเคชันใด ๆ ที่สามารถใช้ข้อมูลใน XML นี้

2.4.2 ความสัมพันธ์ระหว่าง XML และ เว็บเซอร์วิส

เว็บเซอร์วิส สามารถเชื่อมต่อแอพพลิเคชันต่างๆ เข้าด้วยกัน และช่วยแปลงมาตรฐานของแอพพลิเคชันต่างๆ ให้สามารถแบ่งปันข้อมูลระหว่างกันได้ โดยความสามารถในการรวมเอาแอพพลิเคชันต่างๆ นั้น อาศัยการใช้งานของโปรแกรมภาษา XML (extensible markup language) และมาตรฐานด้านการเขียนโปรแกรม XML ที่ถูกใช้ในการแปลงเอกสาร และแอพพลิเคชันต่างๆ ให้สื่อสารกันได้

2.4.2.1 WSDL คือ คู่มือให้กับระบบ เพื่อเรียนรู้วิธีการติดต่อและวิธีการเรียกใช้งานเว็บเซอร์วิสที่ต้องการ โดยเขียนขึ้นตามแบบมาตรฐานไวยากรณ์ของภาษา XML ตัวอย่างโค๊ด ดังแสดงในภาพที่ 6

2.4.2.2 SOAP คือ โพรโตคอลที่อยู่บนพื้นฐานของ XML ทั้งหมด โดยส่งข้อมูลผ่านอินเทอร์เน็ต/เว็บ ในรูปแบบของ XML

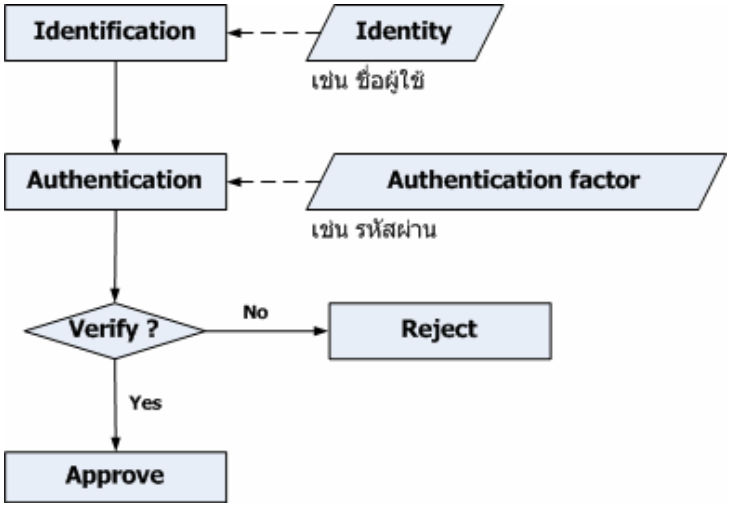
3. การพิสูจน์ตัวตน (Authentication) (ปรัชญา พันธุ์มี และ ดวงแก้ว สวามิภักดิ์ 2547)

การพิสูจน์ตัวตน คือ ขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

3.1 ขั้นตอนการพิสูจน์ตัวตน ในทางปฏิบัติ

3.1.1 การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใครเช่น ชื่อผู้ใช้ (username)

3.1.2 การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง



ภาพที่ 7 แผนผังแสดงกระบวนการการพิสูจน์ตัวตน

จากภาพที่ 7 เป็นแผนผังแสดงกระบวนการพิสูจน์ตัวตน ในขั้นแรกผู้ใช้จะทำการแสดงหลักฐานที่ใช้ในการพิสูจน์ตัวตนต่อระบบ ซึ่งในขั้นนี้คือการระบุตัวตน และในขั้นตอนต่อมาระบบจะทำการตรวจสอบหลักฐานที่ผู้ใช้นำมากล่าวอ้างซึ่งก็คือการพิสูจน์ตัวตน หลังจากระบบได้ทำการตรวจสอบหลักฐานเรียบร้อยแล้วถ้าหลักฐานที่นำมากล่าวอ้างถูกต้องจึงอนุญาตให้เข้าสู่ระบบได้ หากหลักฐานที่นำมากล่าวอ้างไม่ถูกต้องผู้ใช้จะถูกปฏิเสธจากระบบ

3.2 หลักฐานที่ผู้ใช้นำมากล่าวอ้างที่เกี่ยวกับเรื่องของความปลอดภัยนั้นสามารถจำแนกได้ 2 ชนิด

3.2.1 Actual identity คือ หลักฐานที่สามารถบ่งบอกได้ว่าในความเป็นจริงบุคคลที่กล่าวอ้างนั้นเป็นใคร

3.2.2 Electronic identity คือ หลักฐานทางอิเล็กทรอนิกส์ซึ่งสามารถบ่งบอกข้อมูลของบุคคลนั้นได้ แต่ละบุคคลอาจมีหลักฐานทางอิเล็กทรอนิกส์ได้มากกว่า 1 หลักฐาน ตัวอย่างเช่น บัญชีชื่อผู้ใช้ กลไกของการพิสูจน์ตัวตน (Authentication mechanisms) สามารถแบ่งออกได้เป็น 3 คุณลักษณะคือ

3.2.2.1 สิ่งที่คุณมี (Possession factor) เช่น กุญแจหรือเครดิตการ์ด เป็นต้น

3.2.2.2 สิ่งที่คุณรู้ (Knowledge factor) เช่น รหัสผ่าน (password) หรือการใช้หมายเลขประจำตัว (PIN) เป็นต้น

3.2.2.3 สิ่งที่คุณเป็น (Biometric factor) เช่น ลายนิ้วมือ รูปแบบรูม่านตา (retinal patterns) หรือใช้รูปแบบเสียง (voice patterns) เป็นต้น

กระบวนการพิสูจน์ตัวตนนั้นจะนำ 3 ลักษณะข้างต้นมาใช้ในการยืนยันหลักฐานที่นำมากล่าวอ้าง ทั้งนี้ขึ้นอยู่กับระบบ วิธีการที่นำมาใช้เพียงลักษณะอย่างใดอย่างหนึ่ง (Single-factor authentication) นั้นมีข้อจำกัดในการใช้ ตัวอย่างเช่น สิ่งที่คุณมี (Possession factor) นั้นอาจจะสูญหายหรือถูกขโมยได้ สิ่งที่คุณรู้ (Knowledge factor) อาจจะถูกดักฟัง เดา หรือขโมยจากเครื่องคอมพิวเตอร์ สิ่งที่คุณเป็น (Biometric factor) จัดได้ว่าเป็นวิธีที่มีความปลอดภัยสูง อย่างไรก็ตามการที่จะใช้เทคโนโลยีนี้ได้นั้นจำเป็นต้องมีการลงทุนที่สูง เป็นต้น

ดังนั้นจึงได้มีการนำแต่ละคุณลักษณะมาใช้ร่วมกัน (Multi-factor authentication) ตัวอย่างเช่น ใช้สิ่งที่คุณมีกับสิ่งที่คุณรู้มาใช้ร่วมกัน เช่น การใช้ลายมือชื่อร่วมกับการใช้บัตรเครดิต หรือการใช้รหัสผ่านร่วมกับการใช้บัตร ATM เป็นต้น การนำแต่ละลักษณะของการพิสูจน์ตัวตนมาใช้ร่วมกันมากกว่า 1 ลักษณะ จะช่วยเพิ่มประสิทธิภาพในการรักษาความปลอดภัยของข้อมูล

4. การใช้ลายนิ้วมือในการระบุตัวบุคคล (กษิร์พันธ์ มาสกุล 2550)

ลายนิ้วมือของแต่ละคน เริ่มปรากฏขึ้นตั้งแต่เป็นตัวอ่อนอายุ 3 ถึง 4 เดือนในครรภ์มารดา ซึ่งเป็นผิวหนังส่วนที่มีร่อง (Furrow) และมีสัน (Ridge) เอาไว้ใช้สำหรับอำนวยความสะดวกในการหยิบจับสิ่งของ สันและร่องที่ปรากฏนี้มีคุณลักษณะที่สำคัญสองประการ คือ ไม่มีการเปลี่ยนแปลงรูปแบบตามกาลเวลา (แต่อาจเปลี่ยนขนาดได้) และการมีรูปแบบเฉพาะในแต่ละคน

ลายนิ้วมือไม่เปลี่ยนแปลงรูปแบบ (Permanence) ตั้งแต่แรกเกิดจนกระทั่งวันที่เราตาย แต่อาจเปลี่ยนแปลงขนาดได้ตามขนาดร่างกาย เหมือนกับการที่เราวาดรูปไว้บนลูกโป่ง ซึ่งไม่ว่าลูกโป่งจะเล็ก หรือถูกเป่าให้พองใหญ่อย่างไร ก็ยังเป็นรูปเดิมเพียงแต่มีขนาดใหญ่ขึ้นเท่านั้น

ลายนิ้วมือของแต่ละคนนั้นมีลักษณะเฉพาะมากจนกระทั่งแม้แต่ คู่แฝดแท้ (Identical Twin) ก็ยังมีลายนิ้วมือที่แตกต่างกัน (แต่มีรูปแบบ DNA เหมือนกัน) อย่างไรก็ตามรูปแบบของลายนิ้วมือนั้นมีลักษณะความคล้ายกันของคนภายในครอบครัว หรือพูดได้อีกอย่างหนึ่งว่า รูปแบบของลายนิ้วมือมีการถ่ายทอดกันทางพันธุกรรม ซึ่งรูปแบบของลายนิ้วมือ สามารถแบ่งออกได้เป็นประเภทใหญ่ๆ ได้ 3 ประเภท คือแบบลายก้นหอย (Whorl) ลายมัดหวาย (Loop) และลายโค้ง (Arch)

ลายก้นหอย (Whorl)	ลายมัดหวาย (Loop)	ลายโค้ง (Arch)
		

ภาพที่ 8 รูปแบบของลายนิ้วมือ

ที่มา : กษิร์พันธ์ มาสกุล, ไบโอเมทริก (Biometrics) [ออนไลน์], เข้าถึงเมื่อ 6 พฤษภาคม 2550. เข้าถึงได้จาก http://www.spu.ac.th/~bmetric/fp_intro.htm

จากภาพที่ 8 รูปแบบลายนิ้วมือนี้สามารถแบ่งย่อยให้ละเอียดขึ้นไปได้เป็น ลายมัดหวายเอียงขวา (Right Loop) ลายมัดหวายเอียงซ้าย (Left Loop) ลายโค้งสูงแบบกระโจม (Tented Arch) เป็นต้น ลายนิ้วมือแบบลายก้นหอย (Whorl) มีประมาณ 30% ลายนิ้วมือแบบลายมัดหวาย (Loop) มีประมาณ 65% และลายนิ้วมือแบบลายโค้ง (Arch) มีประมาณ 5% การแบ่งลายนิ้วมือออกเป็นหลายประเภทนี้เพื่อวัตถุประสงค์ในการเพิ่มความรวดเร็วในการตรวจสอบลายนิ้วมือ แต่ไม่ได้เป็นสิ่งที่ใช้ในการบอกความเหมือน หรือความแตกต่างระหว่างลายนิ้วมือ แต่เป็นการใช้ลักษณะของสัน (Ridge) ของลายนิ้วมือเช่น การสิ้นสุดของสัน (Ridge Ending) สันแบบลายจุด (Dots) สันที่แตกแขนง (Bifurcations) หรือรูปแบบต่างๆของสันที่เกิดขึ้น เป็นสิ่งที่ใช้ในการเปรียบเทียบลายนิ้วมือ

ตัวอย่างอุปกรณ์ที่ใช้ในการเก็บตัวอย่างลายนิ้วมือ (Fingerprint Scanner)

อุปกรณ์ที่ใช้สแกนลายนิ้วมือในปัจจุบันมีราคาถูกลงมาก และมีแนวโน้มที่จะมีราคาลดลงอย่างต่อเนื่อง ทั้งนี้เนื่องมาจากความแพร่หลาย และการประยุกต์ใช้ลายนิ้วมือกันในงานด้านต่างๆมากขึ้น อุปกรณ์ที่ใช้ในการเก็บตัวอย่างลายนิ้วมือ (ภาพที่ 9) มีอยู่หลายประเภท เช่น

เครื่องสแกนลายนิ้วมือโดยเฉพาะ

เมาส์ที่มีเครื่องสแกนลายนิ้วมือ

คีย์บอร์ดที่มีเครื่องสแกนลายนิ้วมือ

เครื่องสแกนลายนิ้วมือขนาดเล็กแบบ PCMCIA CARD

ภาพที่ 9 ตัวอย่างเครื่องอ่านลายนิ้วมือประเภทต่างๆ
ที่มา : กษิร์พันธ์ มาสกุล, ไบโอเมทริก (Biometrics) [ออนไลน์], เข้าถึงเมื่อ 6 พฤษภาคม 2550. เข้าถึงได้จาก http://www.spu.ac.th/~bmetric/fp_intro.htm

การเลือกใช้อุปกรณ์แต่ละประเภท ขึ้นอยู่กับประเภทงานที่จะนำไปใช้เป็นหลัก เช่น ถ้าใช้การตรวจสอบลายนิ้วมือในการเข้าใช้งานเครือข่ายคอมพิวเตอร์ การใช้เครื่องสแกนลายนิ้วมือที่ติดอยู่กับคีย์บอร์ด หรือเครื่องสแกนที่ติดอยู่กับเมาส์ ก็จะเหมาะสมกว่าเครื่องสแกนลายนิ้วมือประเภทอื่น หรือถ้าการตรวจสอบลายนิ้วมือในการบันทึกเวลาการทำงานของพนักงานก็ควรใช้เครื่องที่ใช้สำหรับสแกนลายนิ้วมือโดยเฉพาะ เป็นต้น

งานวิจัยที่เกี่ยวข้อง

สุจิตรา และคณะ (2550) ได้พัฒนาแบบจำลองการเข้าใช้งานระบบโดยใช้การพิสูจน์ลายพิมพ์นิ้วมือ (System Access Control Model by Verification) ระบบจะทำการเปรียบเทียบ (Fingerprint Matching) เป็นการจับคู่เปรียบเทียบลายพิมพ์นิ้วมือของบุคคลที่ต้องการเข้าใช้ระบบกับลายพิมพ์นิ้วมือของบุคคลนั้นที่เก็บไว้ในฐานข้อมูลว่าเป็นลายพิมพ์เดียวกันหรือไม่ ในการควบคุม

การเข้าใช้ (Access Control) เป็นการตรวจสอบสถานะบุคคล เพื่อพิจารณาอนุญาตให้บุคคลเข้าใช้ระบบได้ แบบการจำลองการเข้าใช้งานระบบได้ถูกออกแบบให้มีการทำงานแบบไคลเอนต์-เซิร์ฟเวอร์ โดยคอมพิวเตอร์ที่ทำหน้าที่เซิร์ฟเวอร์ จะเก็บข้อมูลทั้งหมดของระบบ ส่วนคอมพิวเตอร์ที่ทำหน้าที่ไคลเอนต์ ทำหน้าที่รอรับข้อมูลบุคคลที่ต้องการตรวจสอบ และส่งไปให้เครื่องคอมพิวเตอร์ที่ทำหน้าที่เซิร์ฟเวอร์ต่อไป ซึ่งผลการทดลองระบบสามารถทำงานได้บรรลุตามวัตถุประสงค์และยังมีความสามารถอื่นๆ คือ แบบจำลองสามารถทำงานแบบไคลเอนต์-เซิร์ฟเวอร์ และในส่วนของเครื่องคอมพิวเตอร์ที่ทำหน้าที่เซอร์ฟเวอร์สามารถแสดงข้อมูลการทำงานของเครื่องคอมพิวเตอร์ที่ทำหน้าที่ไคลเอนต์ได้ แบบจำลองสามารถยืนยันตัวบุคคลโดยใช้ลายพิมพ์นิ้วมือโดยรับข้อมูลจากแป้นพิมพ์และเครื่องอ่านลายนิ้วมือนำไปประมวลผล แล้วนำไปเปรียบเทียบกับข้อมูลในฐานข้อมูล และสามารถตรวจสอบการเข้าถึงระบบได้

Fensel and Bussler (2005) กล่าวถึง Web Service Modeling Framework หรือเรียกโดยย่อว่า WSMF เป็นการออกแบบจำลอง WSMF โดยแสดงการทำงานของ e-commerce ให้สามารถทำงานบนเว็บเซอร์วิส ที่เรียกใช้แบบจำลอง WSMF โดยแบบจำลองนี้จะเป็นศูนย์กลางโดยมีหลักการ 2 ส่วนหลักๆ คือ ส่วนแรกจัดการในส่วนของการจำแนกส่วนประกอบของข้อมูลบนความแตกต่างของข้อมูลภายในองค์กร การอธิบายข้อมูลและโปรโตคอลที่ใช้ในการแลกเปลี่ยนข้อมูล ส่วนที่สองเป็นการจัดในส่วนการให้บริการโดยวิเคราะห์ข้อแตกต่างของคำศัพท์และข้อแตกต่างของรูปแบบในการติดต่อ

บทที่ 3
วิธีการดำเนินการวิจัย

วิธีการดำเนินการ การพัฒนาระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส (Web Service) ผู้วิจัยมีแนวคิดในการออกแบบระบบให้สามารถตรวจสอบข้อมูลระหว่างองค์กรได้ โดยใช้หลักการของเว็บเซอร์วิส โดยมีการแบ่งวิธีการดำเนินการ ดังนี้

1. ศึกษาและวิเคราะห์ระบบงานเดิม
2. วิเคราะห์และออกแบบระบบงานใหม่
3. การพัฒนาระบบ
4. การทดสอบและประเมินประสิทธิภาพระบบ

1. ศึกษาและวิเคราะห์งานเดิม

การรวบรวมข้อมูลและผลการรวบรวมข้อมูล ข้อมูลที่นำมาใช้ในการพัฒนาระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส (Development of Access Control System using Web Service)

1.1 การศึกษาและรวบรวมข้อมูล ข้อมูลจากการศึกษา สอบถามข้อมูล และความต้องการจากเจ้าหน้าที่ ซึ่งทำงานฝ่ายอาคารสถานที่ และเจ้าหน้าที่รักษาความปลอดภัยที่ทำหน้าที่ตรวจสอบบุคคล เข้า-ออกอาคาร เพื่อนำมาวิเคราะห์ระบบงานให้ตรงกับความต้องการของผู้ใช้ ซึ่งมีดังนี้

1.1.1 ศึกษาและรวบรวมข้อมูลจากเจ้าหน้าที่ ซึ่งทำงานฝ่ายอาคารสถานที่ และเจ้าหน้าที่รักษาความปลอดภัยที่ทำหน้าที่ตรวจสอบบุคคล เข้า-ออก อาคารของหน่วยงานต่าง ๆ

1.1.2 ศึกษาและรวบรวมข้อมูลการเก็บบันทึกข้อมูลบุคคลเข้า-ออกอาคารในแต่ละวัน

1.1.3 ศึกษาและรวบรวมความต้องการของผู้ติดต่อ

1.2 ขั้นตอนการทำงาน ระบบรักษาความปลอดภัยในการเข้าอาคาร ตามระบบงานเดิม ซึ่งอธิบายเป็นขั้นตอนดังนี้

1.2.1 กรณีการเข้าสถานที่ ต้องทำการแลกบัตรจึงจะสามารถเข้าสถานที่ได้ และบัตรที่ใช้แลกนั้น จะใช้บัตรที่มีรูปหน้าของผู้ติดต่อ ติดอยู่ เพื่อใช้ในการแลกบัตรอนุญาตเข้าสถานที่ ซึ่งในการทำงานในขั้นตอนนี้ไม่สามารถระบุได้ว่าผู้ติดต่อใช้บัตรปลอมหรือบัตรที่ไม่ใช่ของตัวเองได้

1.2.2 ระบบความปลอดภัย เมื่อผ่านขั้นตอนการแลกบัตรแล้วเจ้าหน้าที่รักษาความปลอดภัย จะอนุญาตให้เข้าตัวสถานที่ได้ ในระบบรักษาความปลอดภัยของระบบเดิมนี้ จะมีรูปหน้าของผู้ต้องห้ามในการเข้าอาคารอยู่จำนวนหนึ่ง เป็นรูปที่พิมพ์จากเครื่องพิมพ์ ปัญหาที่พบในระบบความปลอดภัยนี้คือ เจ้าหน้าที่ไม่สามารถใช้รูปภาพผู้ต้องห้ามเข้าอาคารเพียงอย่างเดียวมาตัดสินใจในการห้ามไม่ให้ผู้ติดต่อเข้าสถานที่ได้

1.2.3 การบันทึกข้อมูล เมื่ออนุญาตให้เข้าสถานที่ได้แล้ว เจ้าหน้าที่จะเก็บบัตรที่ผู้ติดต่อได้แลกไว้และนำข้อมูลในบัตรนั้นมาบันทึกลงสมุดบันทึกการเข้าสถานที่ ข้อมูลที่เก็บจะมีดังนี้ เลขที่บัตร ชื่อ สกุล ที่อยู่ และชั้นที่ติดต่อ จะเห็นได้ว่าในการบันทึกลงสมุดนั้นมีความยุ่งยากในการตรวจสอบและค้นหา อีกทั้งจำนวนข้อมูลที่ทำการเก็บบันทึกไม่เพียงพอต่อการติดตามตัวผู้เข้าสถานที่ที่ก่อความเสียหายได้

จากการศึกษาและวิเคราะห์ระบบงานเดิม การรักษาความปลอดภัยในการเข้าสถานที่จะเห็นได้ว่าขั้นตอนของการทำงานยังไม่มีความปลอดภัยเพียงพอ ดังนั้น ผู้วิจัยจึงเกิดแนวคิดในการยืนยันตัวตนและการตรวจสอบข้อมูลบุคคลต้องห้ามเข้าสถานที่ (Blacklist) ระหว่างหน่วยงาน รวมถึงการบันทึกรูปหน้าของผู้ติดต่อขอเข้าสถานที่ทุกครั้งในการเข้าสถานที่ เพื่อเพิ่มประสิทธิภาพในการรักษาความภัยและป้องกันความเสียหายที่อาจเกิดขึ้นได้

2. วิเคราะห์และออกแบบระบบงานใหม่ (Analysis and Design for New System)

2.1 ประโยชน์จากการนำบัตรสมาร์ทการ์ดมาใช้ในระบบ เนื่องจากผู้วิจัยได้มีแนวคิดในการนำบัตรประจำตัวประชาชนแบบสมาร์ทการ์ด เข้ามาใช้ในระบบเพื่อประโยชน์ดังนี้

2.1.1 สามารถยืนยันตัวบุคคลได้ บัตรประจำตัวประชาชนแบบสมาร์ทการ์ด สามารถทำการตรวจสอบลายนิ้วมือของเจ้าของบัตร ทำให้สามารถตรวจสอบได้ว่าผู้ที่ถือบัตรเพื่อใช้ในการเข้าสถานที่ เป็นเจ้าของบัตรจริงหรือไม่

2.1.2 ข้อมูลในบัตรเป็นมาตรฐานเดียวกัน โดยรายละเอียดข้อมูลที่เก็บไว้ใน ชิพ (Chip) ของบัตรมีดังนี้

ตารางที่ 6 ข้อมูลที่จัดเก็บของสำนักทะเบียนกลาง กรมการปกครอง ข้อมูลที่จัดเก็บในชิพบัตรประจำตัวประชาชนแบบสมาร์ทการ์ด ส่วนของสำนักทะเบียนกลาง

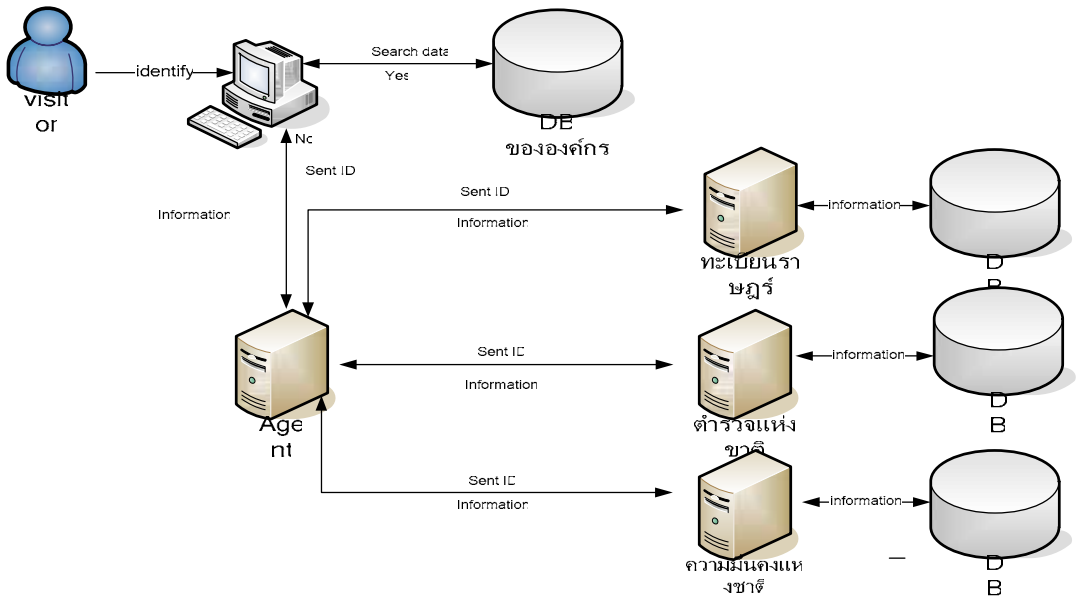
ลำดับ	รายการ	ชนิด	ขนาด	หมายเหตุ
1	เลขประจำตัวประชาชน	N	13	
2	ชื่อ-นามสกุล; คำนำหน้านาม	C	80	
3	ชื่อ-นามสกุล; คำนำหน้านาม (ภาษาอังกฤษ)	C	80	
4	วัน เดือน ปี เกิด	N	8	DDMMYYYY
5	เพศ	N	1	1-ชาย, 2-หญิง
6	สัญชาติ	C	20	
7	ที่อยู่ปัจจุบัน	C	150	
8	ศาสนา	N	1	1.พุทธ, 2.คริสต์, 3. อิสลาม, 4.ซิกข์, 5. พราหมณ์-ฮินดู
9	เลขประจำตัวประชาชนของ บิดา	N	13	
10	ชื่อ-นามสกุล; คำนำหน้านาม ของ บิดา	C	80	
11	สัญชาติของ บิดา	C	20	
12	เลขประจำตัวประชาชนของ บิดา	N	13	
13	ชื่อ-นามสกุล; คำนำหน้านาม ของ บิดา	C	80	
14	สัญชาติของ บิดา	C	20	
15	วันเดือนปี ที่เปลี่ยนชื่อ-นามสกุลล่าสุด	N	8	
16	ชื่อ-นามสกุลเดิมก่อนเปลี่ยนล่าสุด	C	60	DDMMYYYY

ตารางที่ 6 (ต่อ)

ลำดับ	รายการ	ชนิด	ขนาด	หมายเหตุ
17	หมายเลข บัตร/คำร้อง	C	20	ชื่อ#นามสกุล
18	สถานที่/ หน่วยงาน ที่ออกบัตร	C	100	
19	รหัสผู้ออกบัตร (Issuer Code)	C	10	
20	วันเดือนปี ที่ออกบัตร	N	8	
21	วันเดือนปี ที่บัตรหมดอายุ	N	8	DDMMYYYY
22	ภาพใบหน้า	B	5120	DDMMYYYY
23	เลขบัตรประจำตัวประชาชนของคู่สมรส	N	13	
24	ชื่อ-นามสกุลคู่สมรส	C	80	
25	วันเดือนปี ที่สมรส	N	8	DDMMYYYY
26	เลขทะเบียนที่สมรส	C	15	
27	วันเดือน ที่หย่า	N	8	DDMMYYYY
28	เลขทะเบียนที่หย่า	C	15	
29	สถานที่เกิด	C	150	
30	บ้านที่แจ้งย้ายเข้าครั้งแรกหลังการเกิด	C	150	
31	วันเดือนปีที่ย้ายเข้าบ้านครั้งแรกหลังการเกิด	N	8	DDMMYYYY
32	วันที่ปรับปรุงข้อมูล	DATE	8	DDMMYYYY
ข้อมูล ณ วันที่ 10 กุมภาพันธ์ 2547			6368	

ที่มา : สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์/ TU-RAC, การคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในบัตรประจำตัวแบบสมาร์ทการ์ด (Smart Card), (ม.ป.ท., 2547), 38

2.2 แนวคิดในการออกแบบระบบ จากการศึกษาระบบงานปัจจุบันของระบบรักษา ความปลอดภัยในการเข้าสถานที่ พบปัญหาของระบบในเรื่องของความปลอดภัยยังขาดประสิทธิภาพอยู่ ทำให้เกิดแนวคิดในการแก้ไขปัญหา โดยทำการรวบรวมข้อมูล และศึกษาความต้องการที่แท้จริงของกลุ่มผู้ใช้งาน ซึ่งจะทำการออกแบบระบบให้สามารถทำการยืนยันตัวบุคคลได้โดยการตรวจสอบลายนิ้วมือกับข้อมูลลายนิ้วมือที่เก็บในบัตรประชาชนสมาร์ทการ์ด บันทึกข้อมูล รูปหน้า และตรวจสอบบุคคลต้องห้ามเข้าอาคารได้ ตามความต้องการของกลุ่มผู้ใช้ ประกอบกับเทคโนโลยีของเว็บเซอร์วิส มีการพัฒนาขึ้นมาด้วยวัตถุประสงค์คล้ายกันคือ ช่วยให้ทำงานเป็นลักษณะ Interoperability คือมีความสามารถในการทำงานข้ามระบบได้ โดยใช้มาตรฐานกลางทางเทคนิคที่ทำให้การแลกเปลี่ยนและเรียกใช้ข้อมูลข้ามระบบที่มีความแตกต่างกันทั้ง ฮาร์ดแวร์ และซอฟต์แวร์ ซึ่งมีความยืดหยุ่นในการใช้งานและการพัฒนา ประกอบกับเป็นเทคโนโลยีที่ยอมรับและได้รับการสนับสนุนจากหลาย ๆ องค์กร รวมทั้งยังมีเครื่องมือที่ช่วยพัฒนามากมาย เช่น Microsoft.Net Framework, Sun Open Environment, IBM Service Toolkit ดังนั้น จึงนำเอาปัญหาจากการศึกษาและรวบรวม รวมทั้งนำเอาเทคโนโลยี และเครื่องมือที่ได้ศึกษา และมีความสอดคล้องกันนำมาพัฒนาระบบการแลกเปลี่ยนข้อมูลระหว่างกัน เพื่อเพิ่มประสิทธิภาพให้กับระบบรักษาความปลอดภัย เป็นหลักโดยภาพรวมของระบบอธิบายในภาพที่ 10



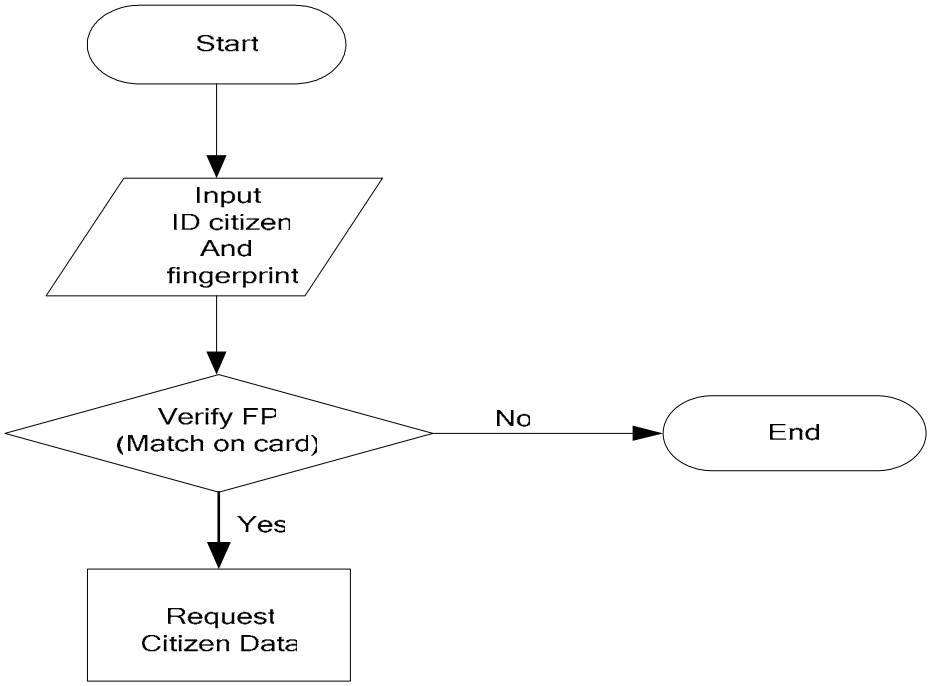
ภาพที่ 10 ภาพรวมของระบบการทำงาน

จากภาพที่ 10 หลักการทำงานของระบบคือ ในการเข้าสถานที่ผู้ติดต่อต้องทำการยืนยันตัวตน โดยการสแกนลายนิ้วมือเปรียบเทียบกับข้อมูลลายนิ้วมือในบัตรประจำตัวประชาชนของผู้ติดต่อ ในกรณีลายนิ้วมือไม่ตรงกันระบบจะไม่อนุญาตให้เข้าสถานที่ได้ แต่ในทางตรงกันข้ามลายนิ้วมือตรงกัน ระบบจะส่งรหัสบัตรประจำตัวประชาชน 13 หลัก ไปเรียกใช้บริการข้อมูลประจำตัวประชาชนของระบบเว็บเซอร์วิสสำนักงานทะเบียนราษฎร์ เพื่อนำข้อมูลมาแสดงบนหน้าจอของระบบ หลังจากนั้นระบบจะทำการตรวจสอบผู้ติดต่อว่าเป็นผู้ต้องห้ามเข้าสถานที่หรือไม่โดยจะทำการตรวจสอบจากฐานข้อมูลทั้งหมด 3 ฐานข้อมูล คือ ฐานข้อมูลระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส ฐานข้อมูลระบบเว็บเซอร์วิสสำนักงานตำรวจแห่งชาติ และฐานข้อมูลระบบเว็บเซอร์วิสสำนักงานความมั่นคงแห่งชาติ โดยหลักของการตรวจสอบคือ ถ้ามีการตรวจสอบพบว่าข้อมูลผู้ติดต่อตรงกับฐานข้อมูลผู้ต้องห้ามเข้าสถานที่ในระบบใด ระบบจะไม่อนุญาตให้เข้าสถานที่ได้ แต่ถ้าข้อมูลผู้ติดต่อไม่ตรงกับฐานข้อมูลผู้ต้องห้ามเข้าสถานที่ของระบบใดเลย ระบบจะอนุญาตให้เข้าสถานที่ได้ โดยก่อนการเข้าสถานที่ระบบจะทำการบันทึกรูปหน้าผู้ติดต่อลงฐานข้อมูลด้วย โดยมีการออกแบบระบบฐานข้อมูล ดังภาคผนวก ก ตารางฐานข้อมูลระบบ

3. การพัฒนาระบบ

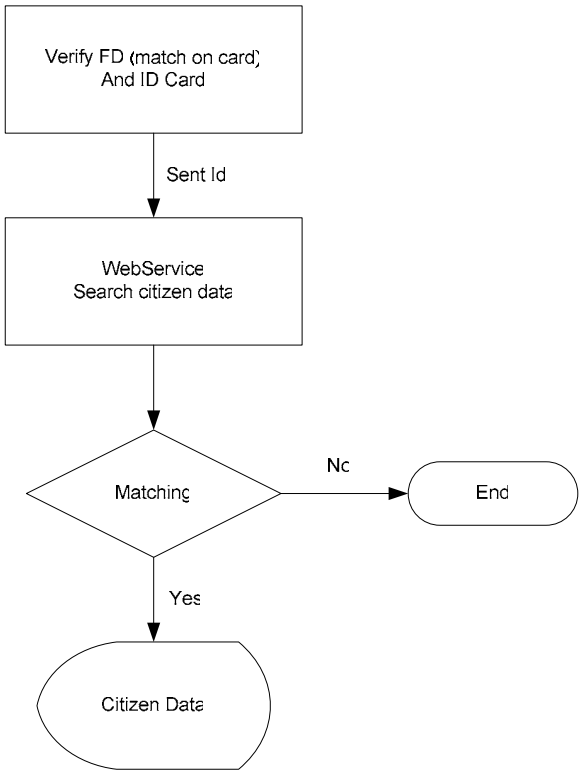
3.1 ขั้นตอนการพัฒนาระบบ

3.1.1 ระบบการยืนยันตัวบุคคล ผู้ติดต่อต้องนำบัตรประจำตัวประชาชนแบบสมาร์ทการ์ดมาแสดงต่อเจ้าหน้าที่เพื่อขอเข้าสถานที่ จากนั้นเจ้าหน้าที่จะทำการตรวจสอบบัตร โดยการตรวจสอบลายนิ้วมือของผู้ติดต่อว่าตรงกับลายนิ้วมือในบัตรหรือไม่ โดยใช้เครื่องอ่านบัตรประจำตัวประชาชนแบบสมาร์ทการ์ดและระบุตัวตนด้วยลายนิ้วมือ IRIS ST-BIOCard Reader ที่เชื่อมต่อกับระบบ ถ้าลายนิ้วมือไม่ตรงกันจะไม่อนุญาตให้เข้าสถานที่ได้ โดยภาพของการทำงานในขั้นตอนการยืนยันตัวบุคคลเป็นดังภาพที่ 11



ภาพที่ 11 การยืนยันตัวตนด้วยการสแกนลายนิ้วมือ

3.1.2 การค้นหาข้อมูลผู้ติดต่อ โดยระบบจะใช้รหัสบัตรประชาชนค้นหาจากสำนักงานทะเบียนราษฎร์ผ่านระบบเว็บเซอร์วิส เพื่อใช้บริการข้อมูลประจำตัวผู้ติดต่อโดยค้นหาจากเลขบัตรประจำตัวประชาชน เพื่อนำมาแสดงผลใน Windows Application ดังภาพที่ 12



ภาพที่ 12 การค้นหาข้อมูลประจำตัวประชาชน

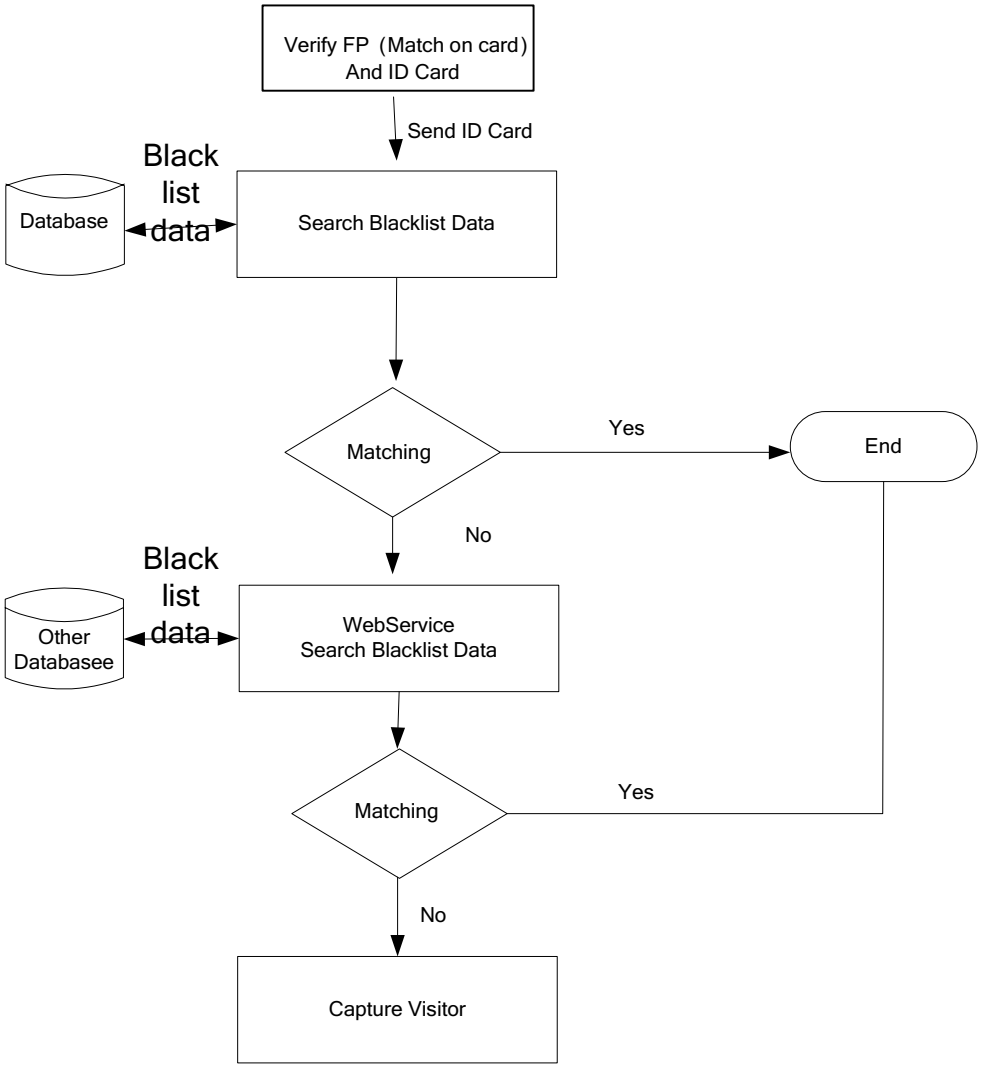
3.1.3 การตรวจสอบข้อมูลผู้ต้องห้ามเข้าสถานที่ เป็นขั้นที่ใช้ตรวจสอบว่าผู้ติดต่อเป็นบุคคลต้องห้ามเข้าสถานที่หรือไม่ โดยจะทำการค้นหาทั้งหมด 3 ฐานข้อมูล ได้แก่

3.1.3.1 ฐานข้อมูลระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส

3.1.3.2 ฐานข้อมูลสำนักงานความมั่นคงแห่งชาติ เป็นเว็บเซอร์วิสที่ให้บริการข้อมูลผู้ต้องห้ามเข้าสถานที่ ที่จำลองขึ้นโดยผู้วิจัย

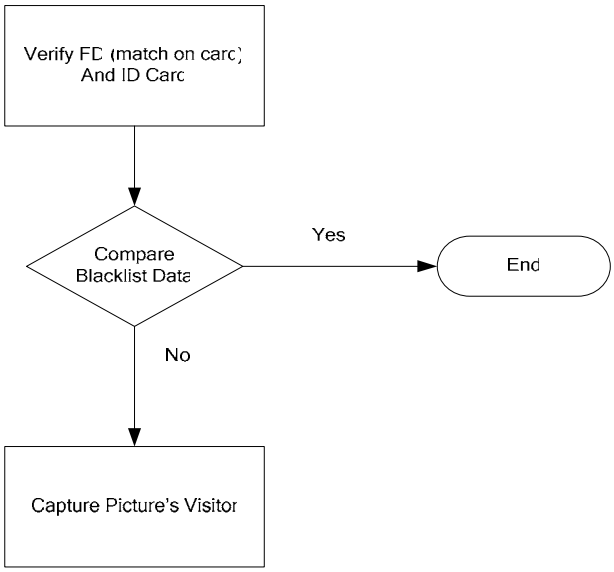
3.1.3.3 ฐานข้อมูลสำนักงานตำรวจแห่งชาติเป็นเว็บเซอร์วิสที่ให้บริการข้อมูลผู้ต้องห้ามเข้าสถานที่ ที่จำลองขึ้นโดยผู้วิจัย

โดยฐานข้อมูลระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิสสามารถเพิ่มข้อมูลบุคคลต้องห้ามเข้าสถานที่ได้ และทุกครั้งที่มีการตอบสอบพบผู้ติดต่อที่เป็นบุคคลต้องห้ามในฐานข้อมูลสำนักงานความมั่นคงหรือสำนักงานตำรวจแห่งชาติ ระบบจะทำการบันทึกข้อมูลนั้นลงฐานข้อมูลระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิสในการตรวจสอบข้อมูลผู้ติดต่อว่าเป็นผู้ต้องห้ามเข้าสถานที่ หรือไม่ จะทำการตรวจสอบทั้ง 3 ฐานข้อมูล หากมีข้อมูลผู้ติดต่อตรงกับฐานข้อมูลใด ระบบจะไม่อนุญาตให้เข้าสถานที่ได้ดังภาพที่ 13



ภาพที่ 13 การตรวจสอบข้อมูลผู้ต้องห้ามเข้าสถานที่

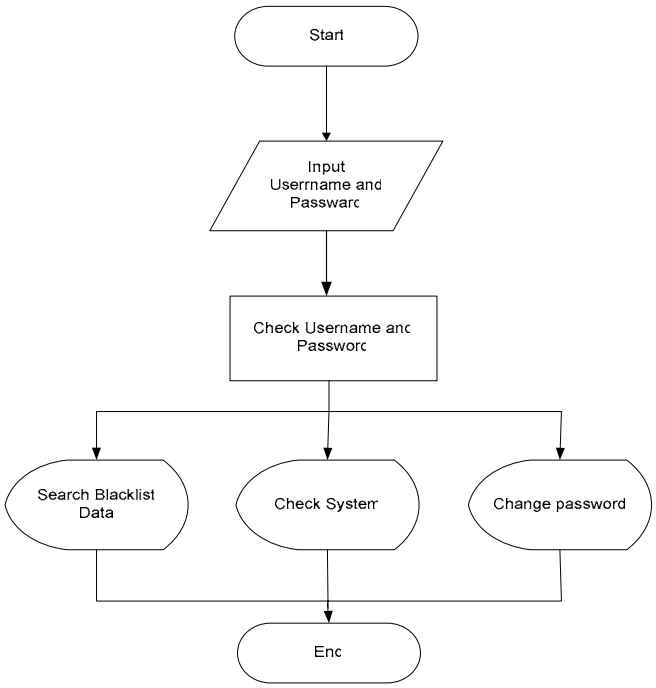
3.1.3.4 การบันทึกข้อมูลผู้เข้าสถานที่ หลังจากระบบทำการตรวจสอบข้อมูลผู้ติดต่อกับฐานข้อมูลผู้ต้องห้ามเข้าสถานที่ หากข้อมูลผู้ติดต่อตรงกันจะไม่อนุญาตให้เข้าสถานที่ ในทางตรงกันข้ามข้อมูลผู้ติดต่อไม่ตรงกันข้อมูลผู้ต้องห้ามเข้าสถานที่ ระบบจะทำการถ่ายรูปหน้าผู้ติดต่อไว้ก่อนการเข้าสถานที่ และบันทึกเก็บไว้ในฐานข้อมูลระบบดังภาพที่ 14



ภาพที่ 14 แสดงการบันทึกรูปหน้าผู้ติดต่อขอเข้าสถานที่

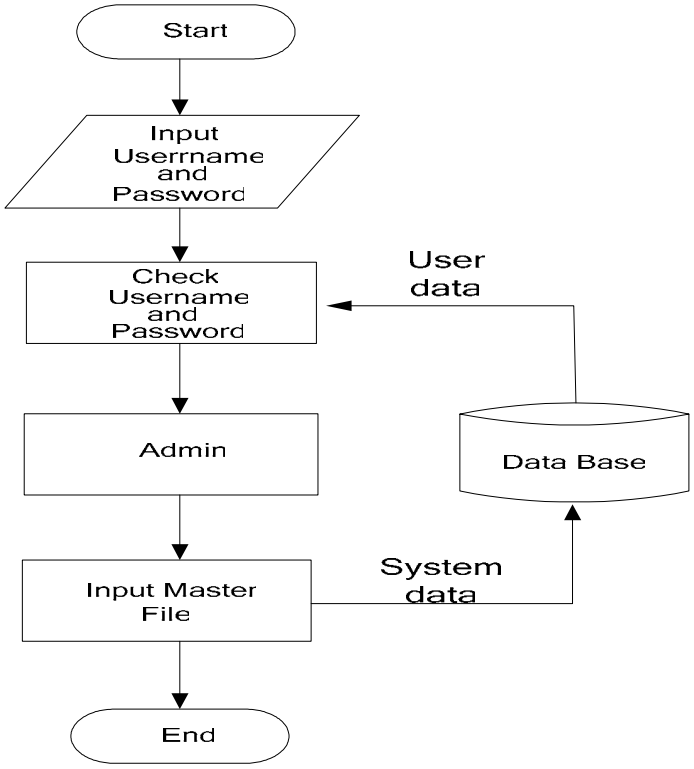
3.2 ขั้นตอนการทำงานของ Process ต่าง ๆ ในระบบ มีดังต่อไปนี้

3.2.1 ขั้นตอนการ login เข้าระบบ เจ้าหน้าที่กรอก ชื่อผู้ใช้และรหัสผู้ใช้ อธิบายได้ดังภาพที่ 15



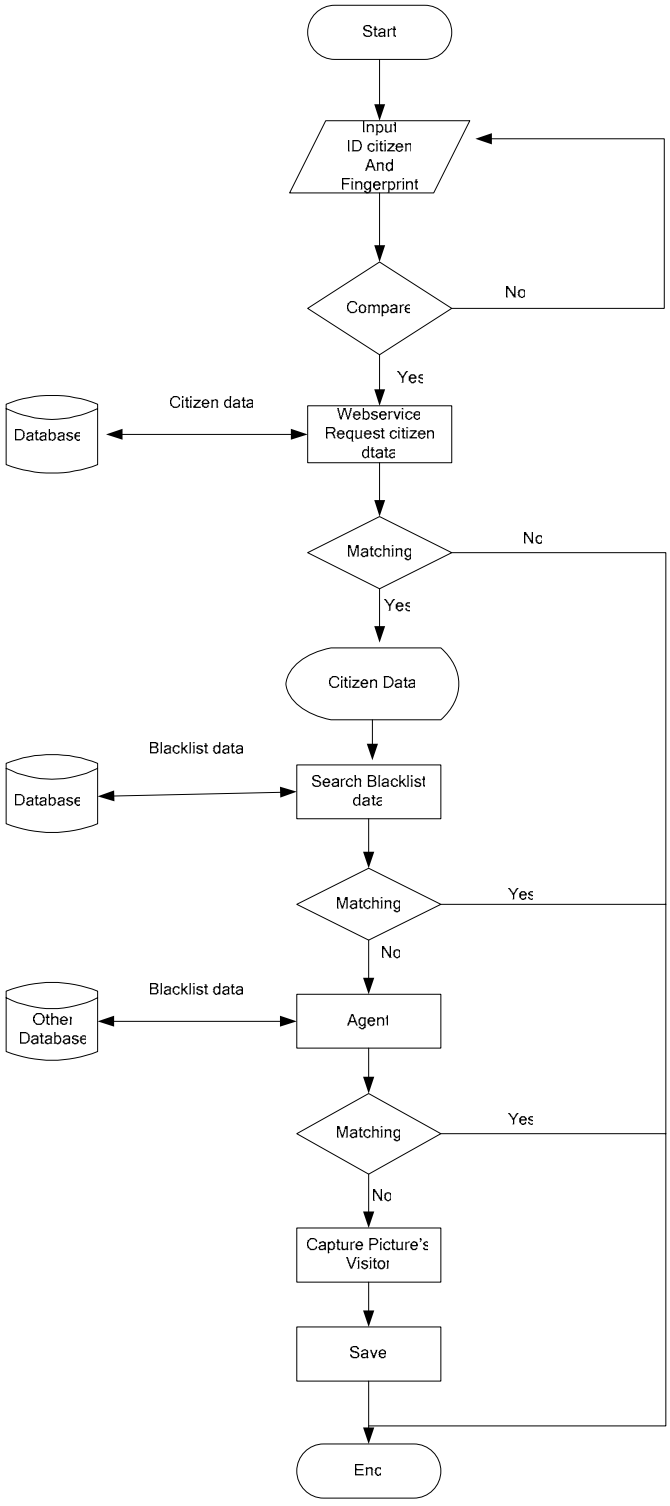
ภาพที่ 15 แสดงขั้นตอนการ Login เข้าสู่ระบบ

3.2.2 ขั้นตอนการนำข้อมูลเข้าสู่ Database ในขั้นตอนนี้ ผู้ใช้ที่มีสถานะที่เป็น Admin เท่านั้นที่สามารถทำการนำข้อมูลเข้า Database ของระบบได้ ดังภาพที่ 16



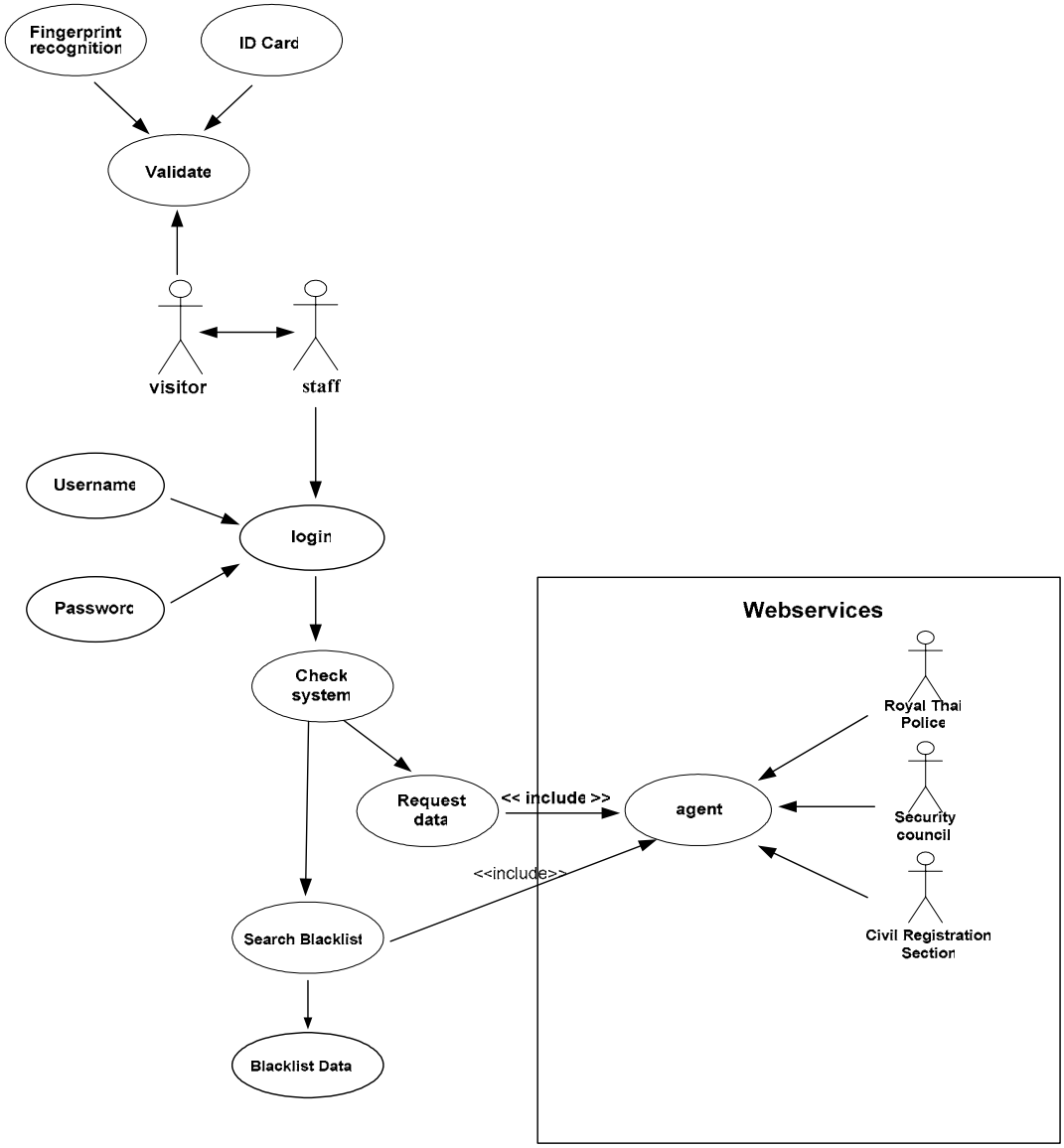
ภาพที่ 16 แสดงขั้นตอนการทำงานของการนำข้อมูลเข้าสู่ Database

3.2.3 ขั้นตอนการทำงานทั้งหมดของระบบโดยรวม จะอธิบายดังภาพที่ 17



ภาพที่ 17 ขั้นตอนการทำงานของระบบ

จากการดำเนินการพัฒนาระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิสนั้น จะเน้นการเรียกใช้และตรวจสอบข้อมูลข้ามองค์กร ในการทดสอบการเรียกใช้และตรวจสอบข้อมูลข้ามองค์กร ผู้วิจัยได้สร้าง Application ด้วยโปรแกรม Visual Basic.Net2005 (VB.Net) ในการพัฒนา โดยอธิบายขั้นตอนการใช้งานโปรแกรม ดังภาคผนวก ก คู่มือการใช้โปรแกรม ซึ่งมีผลทำให้ระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส มีความปลอดภัยและน่าเชื่อถือมากขึ้น ซึ่งมีกระบวนการทำงานดังภาพที่ 18

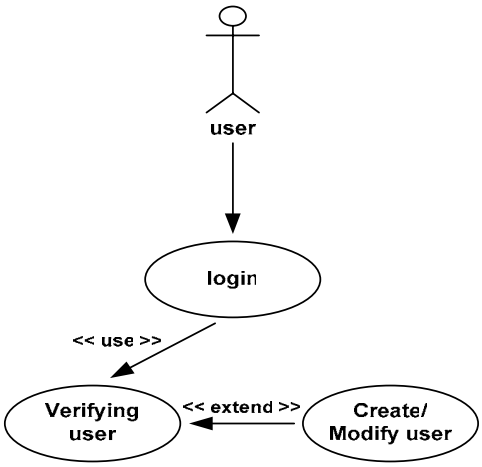


ภาพที่ 18 แสดง Use Case การพัฒนาระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส

จากภาพที่ 18 Use Case แสดงการพัฒนาระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส สามารถอธิบายส่วนประกอบต่าง ๆ ได้ดังนี้

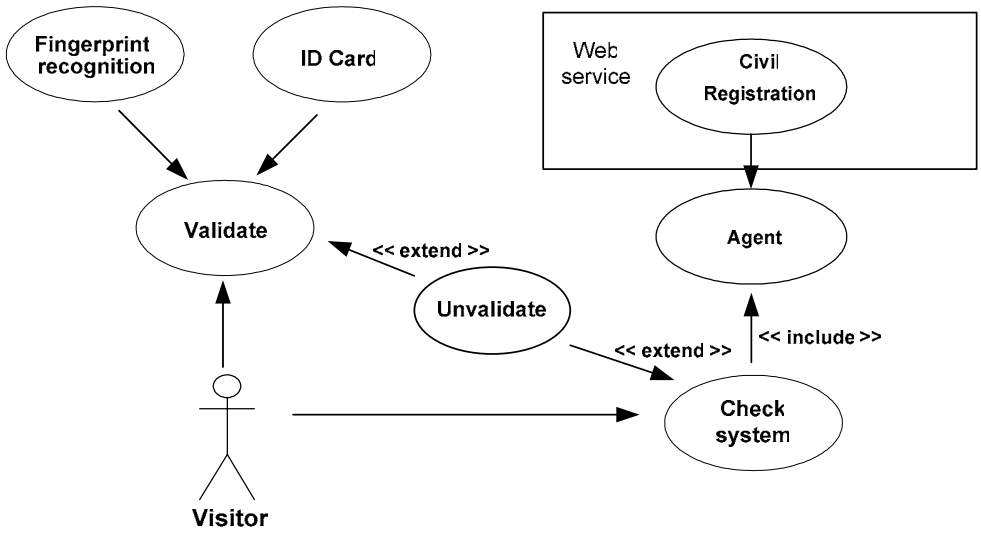
1. Visitor คือ ผู้ติดต่อขอเข้าสถานที่
2. Validate user คือ ระบบยืนยันตัวบุคคล
3. ID Card คือ เช็ครหัสบัตรประจำตัวประชาชน
4. Fingerprint recognition คือ การสแกนลายนิ้วมือ
5. Staff คือ เจ้าหน้าที่ควบคุมระบบตรวจสอบบุคคลเข้า-ออก
6. Login คือ การตรวจสอบสถานะผู้เข้าใช้ระบบ
7. Username คือ ชื่อผู้เข้าใช้ระบบ
8. Password คือ รหัสส่วนตัวผู้เข้าใช้ระบบ
9. Check System คือ ระบบตรวจสอบบุคคลเข้า-ออก
10. Request Data คือ ค้นหาข้อมูลประวัติผู้ติดต่อขอเข้าสถานที่
11. Search Black คือ ค้นหาข้อมูลผู้ต้องห้ามเข้าสถานที่
12. agent คือ การค้นหาข้อมูลประจำตัวประชาชนและข้อมูลผู้ต้องห้ามเข้าสถานที่ จากองค์กรให้บริการข้อมูลประจำตัวประชาชนและข้อมูลผู้ต้องห้ามเข้าสถานที่ เชื่อมโยงแลกเปลี่ยนข้อมูลกันผ่านระบบเว็บเซอร์วิส
13. Royal Thai Police คือ สำนักงานตำรวจแห่งชาติที่ให้บริการข้อมูลผู้ต้องห้ามเข้าสถานที่ เชื่อมโยงแลกเปลี่ยนข้อมูลกันผ่านระบบเว็บเซอร์วิส
14. Security council คือ สำนักงานความมั่นคงแห่งชาติ ให้บริการข้อมูลผู้ต้องห้ามเข้าสถานที่ เชื่อมโยงแลกเปลี่ยนข้อมูลกันผ่านระบบเว็บเซอร์วิส
15. Civil Registration Section คือ ระบบทะเบียนราษฎร์ที่ให้บริการข้อมูลประจำตัวประชาชนผ่านระบบเว็บเซอร์วิส
16. Blacklist data คือ ข้อมูลผู้ต้องห้ามเข้าสถานที่ ของระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส

โปรแกรมระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส เป็นโปรแกรมที่ผู้ใช้ระบบต้องทำการลงทะเบียนเพื่อเข้าใช้ระบบโดยกรอกชื่อผู้ใช้และรหัสผู้ใช้ มีการกำหนดสถานะผู้ใช้เป็น 2 สถานะคือ สถานะ Admin และ User โดยสถานะ Admin สามารถทำการเพิ่มและแก้ไขข้อมูลหลักของระบบได้ ส่วนสถานะ User จะทำงานได้เฉพาะส่วนที่ Admin กำหนดเท่านั้น และผู้ใช้ระบบสามารถแก้ไขข้อมูลส่วนตัวของตัวเองได้ ดังภาพที่ 19



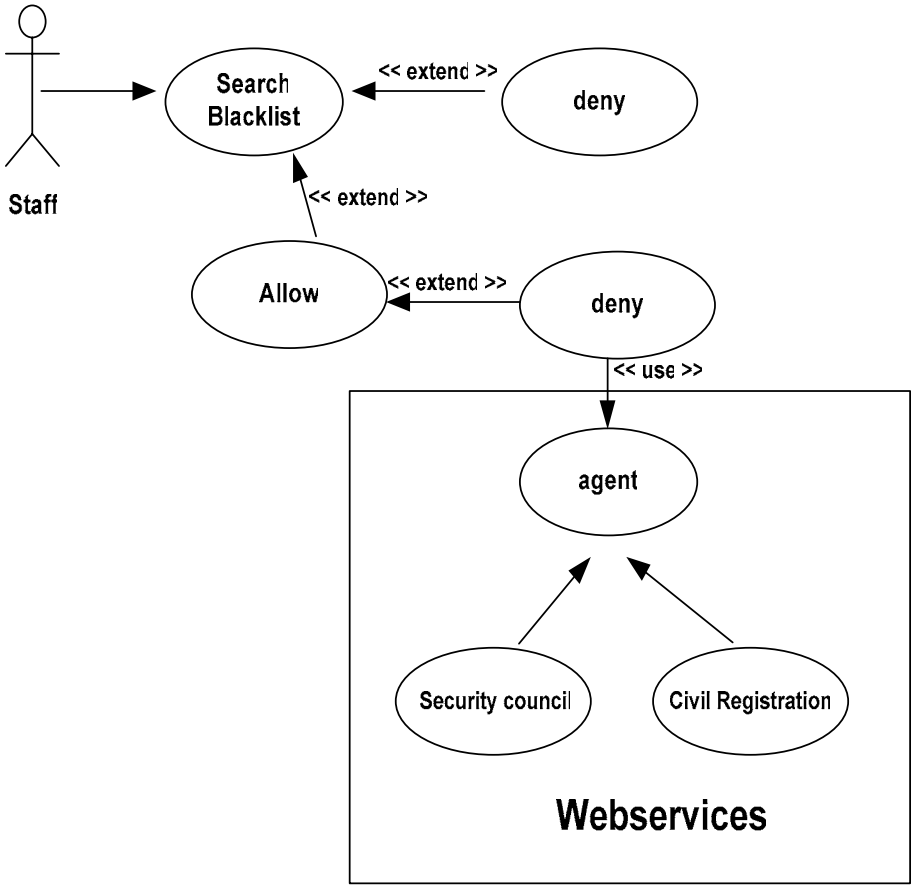
ภาพที่ 19 แสดง use cases การเข้าสู่ระบบ

เมื่อเจ้าหน้าที่การ login เข้าระบบแล้ว เมื่อมีผู้ติดต่อขอเข้าสถานที่ เจ้าหน้าที่จะใช้ระบบทำการตรวจสอบว่าบัตรเป็นของจริงและเป็นของตัวเองหรือไม่ ด้วยขั้นตอนการยืนยันตัวบุคคลโดยใช้การสแกนลายนิ้วมือเปรียบเทียบกับข้อมูลลายนิ้วมือในบัตร ว่าตรงกันหรือไม่ ถ้าไม่ตรงกันจะไม่อนุญาตให้เข้าอาคารได้ แต่ถ้าข้อมูลตรงกันระบบจะทำงานในขั้นตอนต่อไป คือการเรียกใช้บริการข้อมูลประจำตัวประชาชน จากระบบเว็บเซอร์วิสสำนักงานทะเบียนราษฎร์ โดยระบบจะส่งเลขประจำตัวประชาชนเป็นพารามิเตอร์เพื่อใช้ในการค้นหาข้อมูลแล้วนำมาแสดงผลในหน้าจอระบบการตรวจสอบบุคคลเข้า-ออกสถานที่ ดังภาพที่ 20



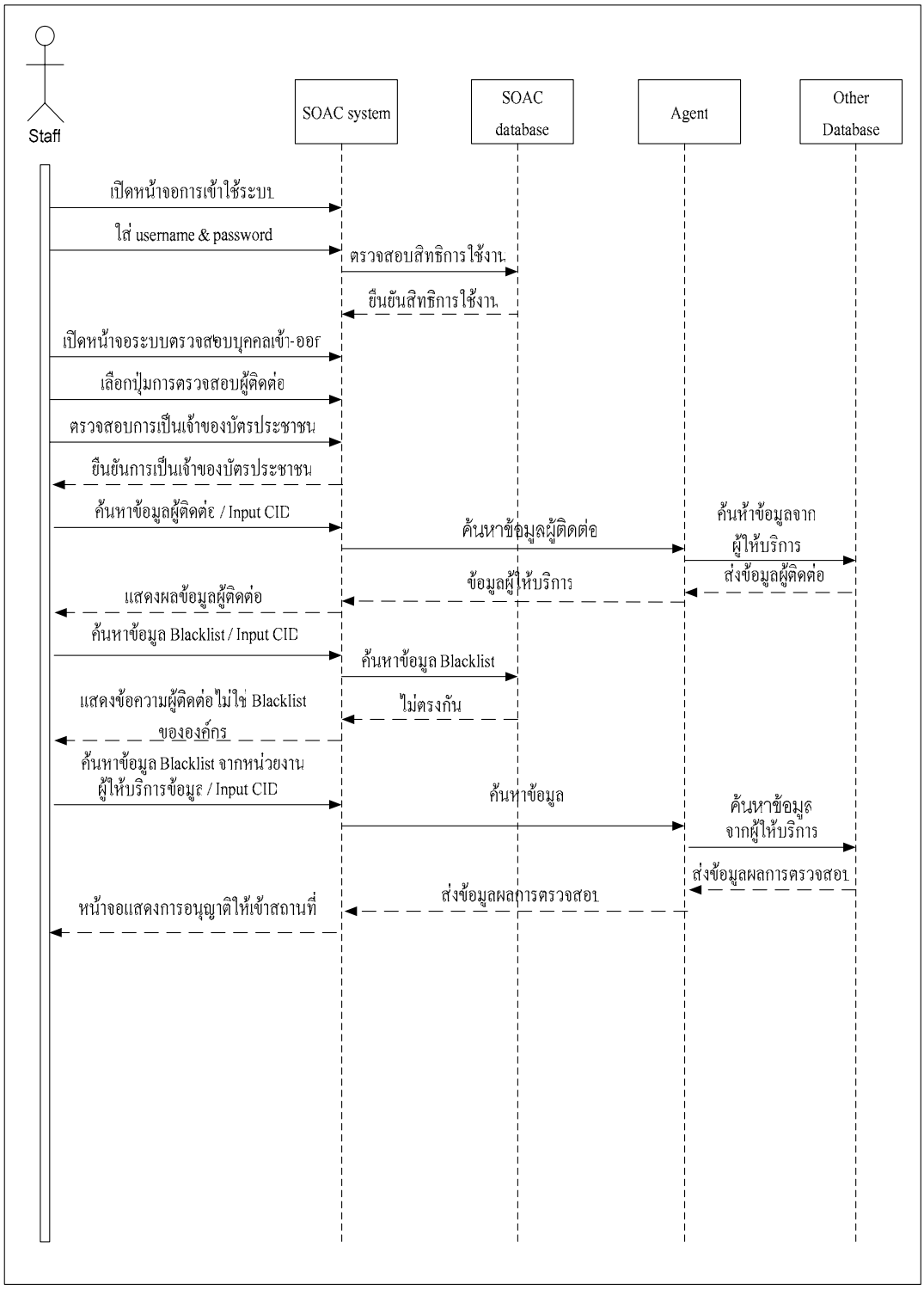
ภาพที่ 20 แสดง Use Cases การเรียกใช้บริการข้อมูลประจำตัวประชาชน

การตรวจสอบข้อมูลผู้ติดต่อว่าตรงกับข้อมูลผู้ต้องห้ามเข้าสถานที่ ของระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส ระบบสำนักงานความมั่นคงแห่งชาติ และระบบสำนักงานตำรวจแห่งชาติ หรือไม่ หากผู้ติดต่อขอเข้าสถานที่มีข้อมูลตรงกับข้อมูลผู้ต้องห้ามเข้าสถานที่ ของระบบใดระบบหนึ่งจะไม่อนุญาตให้มีการเข้าสถานที่ได้ ดังภาพที่ 21



ภาพที่ 21 แสดง Use Cases การตรวจสอบข้อมูลผู้ต้องห้ามเข้าสถานที่

การทำงานของระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส ที่มีการยืนยันตัวบุคคล การเรียกใช้บริการข้อมูลประจำตัวประชาชน และการตรวจสอบข้อมูลผู้ต้องห้ามเข้าสถานที่ จะอธิบายดังภาพที่ 22



ภาพที่ 22 แสดง Sequence diagram ของระบบการเข้า-ออกสถานที่

3.3 เครื่องมือที่ใช้ในการพัฒนาระบบ

3.3.1 ฮาร์ดแวร์ (Hardware)

3.3.1.1 Laptop

1) Intel Core DUO processor ความเร็ว 1.6 GHz

2) หน่วยความจำ ขนาด 2 GB ฮาร์ดดิสก์ ขนาด 80 GB

3.3.1.2 เครื่องอ่านบัตรประชาชนแบบสมาร์ทการ์ดและพิสูจน์เอกลักษณ์ตัวบุคคลด้วยลายนิ้วมือ รุ่น IRIS XP-BIOCARDREADER

3.3.1.3 กล้อง Web Cam V-Gear รุ่น TalkCam1.1

3.3.2 ซอฟต์แวร์ (Software)

3.3.2.1 ระบบปฏิบัติการ Microsoft Windows XP Professional SP2

3.3.2.2 Visual Studio .NET 2005 (VB.NET)

3.3.2.3 ระบบจัดการฐานข้อมูล Microsoft Access 2003

3.3.2.3 Internet Information Service 5.1 (IIS 5.1)

4. การทดสอบและประเมินประสิทธิภาพระบบ

ผู้วิจัยจะทำการประเมินประสิทธิภาพการทำงานของระบบโดยใช้หลักการทางสถิติโดยออกแบบใบประเมินประสิทธิภาพระบบ ดังภาคผนวก ข แบบประเมินผลการทดสอบระบบ ทั้งนี้ผู้วิจัยได้ใช้แบบในการวิเคราะห์ตามแนวคิดของเบสท์ (Best 1970) เข้ามาช่วยในการสรุปผลการประเมินประสิทธิภาพของระบบงานที่ได้พัฒนาขึ้นและกำหนดระดับของการวัดประสิทธิภาพเป็นช่วงคะแนนได้ 5 ระดับ ตามแสดงในตารางที่ 7

ตารางที่ 7 เกณฑ์การให้คะแนนของแบบประเมินประสิทธิภาพของระบบงาน

ระดับเกณฑ์การให้คะแนน		ความหมาย
เชิงคุณภาพ	เชิงปริมาณ	
มาก	4.6 – 5	ระบบที่พัฒนาอยู่ในระดับดีมาก
ดี	3.6 – 4.59	ระบบที่พัฒนาอยู่ในระดับดี
พอใช้	2.6 – 3.59	ระบบที่พัฒนาอยู่ในระดับพอใช้
ปรับปรุง	1.6 – 2.59	ระบบที่พัฒนาอยู่ในระดับที่ควรปรับปรุง
ไม่เหมาะสม	1.0 -1.59	ระบบที่พัฒนาอยู่ในระดับไม่เหมาะสม

ที่มา : Best, John W. Research in Education**.** Englewood Cliffs, New Jersey : Pretice-Hall, Inc. 1970.

โดยการประเมินประสิทธิภาพของระบบจะประเมินในด้านการใช้งานระบบและด้านการทำงานของระบบดังนี้

4.1 ขั้นตอนการทำงานเป็นระบบง่ายต่อการใช้งานไม่ซับซ้อน

4.2 ข้อมูลครบถ้วนตามความต้องการ

4.3 การประมวลผลจากระบบได้ผลลัพธ์ถูก ต้องตามเหตุการณ์จริง

4.4 รูปแบบของหน้าจอสีตัวอักษะและรูปภาพที่ใช้ประกอบมีความเหมาะสม

4.5 เป็นประโยชน์ต่อการนำมาใช้ในระบบรักษาความปลอดภัย

4.6 สะดวกรวดเร็วในการสืบค้นข้อมูล

4.7 ข้อมูลที่สืบค้นมีความถูกต้อง

4.8 ข้อมูลที่จัดเก็บมีความถูกต้อง

4.9 ความถูกต้องในการแก้ไขข้อมูล

4.10 ความเร็วในการประมวลผลข้อมูล

4.11 ความเร็วในการรับส่งข้อมูล

บทที่ 4
ผลการดำเนินงาน

การพัฒนาระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส ประกอบด้วยเว็บเซอร์วิสที่ผู้พัฒนาได้จำลองขึ้นมีทั้งหมด 3 หน่วยงาน ได้แก่

1. ระบบเว็บเซอร์วิสสำนักงานทะเบียนราษฎร์ เปิดให้บริการข้อมูลประจำตัวประชาชน
2. ระบบเว็บเซอร์วิสสำนักงานความมั่นคงแห่งชาติ เปิดให้บริการ การตรวจสอบข้อมูล Blacklist
3. ระบบเว็บเซอร์วิสสำนักงานตำรวจแห่งชาติเปิดให้บริการ การตรวจสอบข้อมูล Blacklist

1. ระบบเว็บเซอร์วิสสำนักงานทะเบียนราษฎร์ เปิดให้บริการข้อมูลประจำตัวประชาชน

เว็บเซอร์วิสของระบบสำนักงานทะเบียนราษฎร์เปิดให้บริการดังนี้

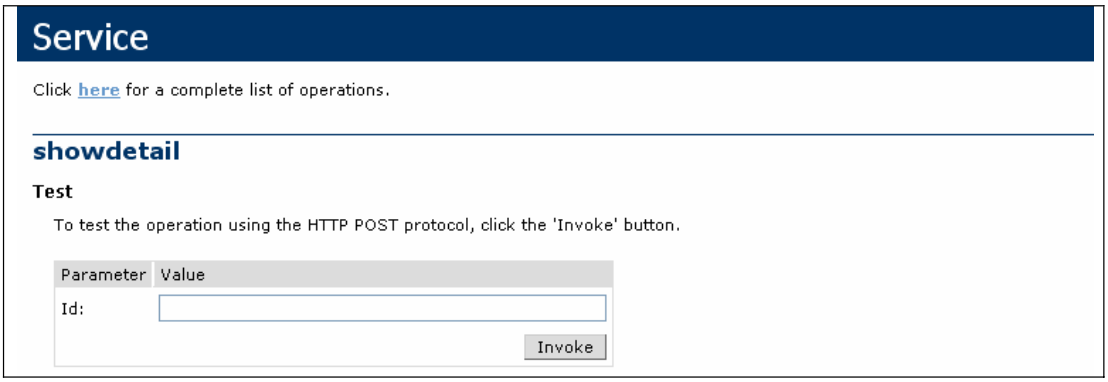
เซอร์วิสการบริการข้อมูลประจำตัวประชาชน

สถานที่เปิดให้บริการ : สำนักงานทะเบียนราษฎร์

ชื่อเซอร์วิส : Showdetail

ข้อมูลที่รับเข้า : Id (หมายเลขบัตรประจำตัวประชาชน)

ผลที่ได้ : ข้อมูลประจำตัวประชาชน



ภาพที่ 23 แสดงเซอร์วิส Showdetail

จากภาพที่ 23 การพัฒนาระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิสทำการเรียกใช้เซอร์วิส Showdetail โดยส่งค่าพารามิเตอร์เป็นหมายเลขบัตรประจำตัวประชาชนของผู้ติดต่อขอเข้าสถานที่ และถ้าไม่มีข้อผิดพลาดระบบเว็บเซอร์วิสสำนักงานทะเบียนราษฎร์จะส่งค่าข้อมูลประจำตัวประชาชนของผู้ติดต่อนั้น โดยแสดงข้อมูลที่ส่งมาในรูปแบบโครงสร้างของเอกสารXML ดังภาพที่ 24

```
<?xml version="1.0" encoding="utf-8" ?>
- <UserClassDetial xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://tempuri.org/
  <cid>3730200101968</cid>
  <pname>นาย</pname>
  <fmane>สมเกียรติ</fmane>
  <lname>ดอนทองแดง</lname>
  <birthday>4/4/1980</birthday>
  <citizenship>ไทย</citizenship>
  <nationality>ไทย</nationality>
  <occupation>นักศึกษา</occupation>
  <bloodgrp>AB</bloodgrp>
  <religion>คริส</religion>
  <addrpart>49</addrpart>
  <moopart>2</moopart>
  <amppart>กำแพงแสน</amppart>
  <tmbpart>สระสี่มุม</tmbpart>
  <road>-</road>
  <chwpart>นครปฐม</chwpart>
  <po_code>73140</po_code>
  <hometel>0832086824</hometel>
  <sex>ชาย</sex>
  <marrystatus>โสด</marrystatus>
  <fathername>นายสมชาย</fathername>
  <fatherlname>ดอนทองแดง</fatherlname>
  <mathername>นางหมูแดง</mathername>
  <matherlname>ดอนทองแดง</matherlname>
</UserClassDetial>
```

ภาพที่ 24 แสดงโครงสร้างเอกสาร XML ของเซอร์วิส Showdetail

2. ระบบเว็บเซอร์วิสสำนักงานความมั่นคงแห่งชาติ เปิดให้บริการการตรวจสอบข้อมูลผู้ต้องห้าม

เว็บเซอร์วิสของระบบสำนักงานความมั่นคงแห่งชาติเปิดให้บริการดังนี้

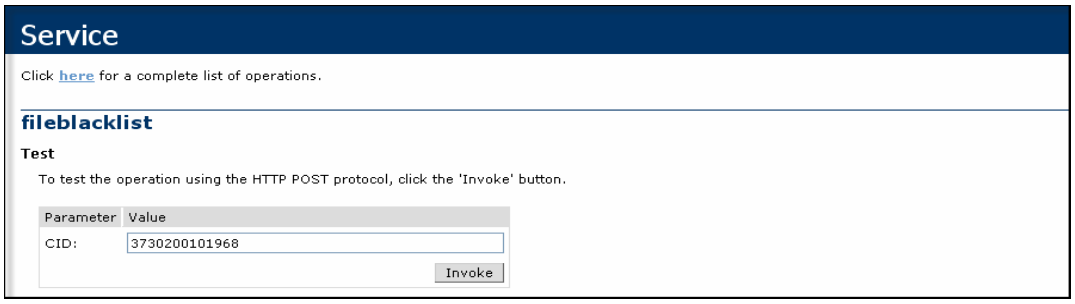
เซอร์วิสการตรวจสอบข้อมูลผู้ต้องห้ามเข้าสถานที่

ส่วนที่เปิดให้บริการ : สำนักงานความมั่นคงแห่งชาติ

ชื่อเซอร์วิส : fileblacklist

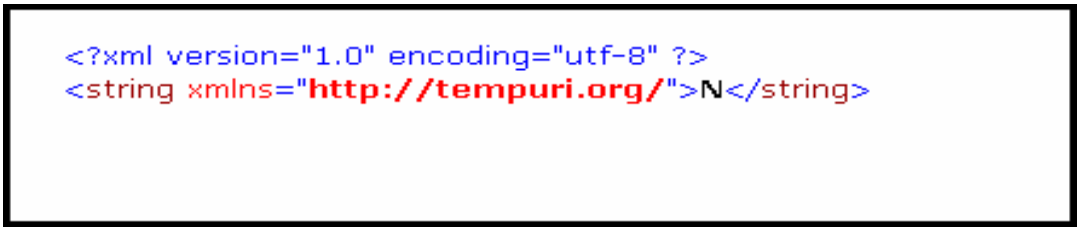
ข้อมูลที่รับเข้า : CID (หมายเลขบัตรประจำตัวประชาชน)

ผลที่ได้ : เป็นค่าของการตรวจสอบ “Y” คือค่าที่ตรวจสอบพบในฐานข้อมูล “N” คือค่าที่ไม่มีการตรวจพบในฐานข้อมูล



ภาพที่ 25 แสดงเซอร์วิส fileblacklist

จากภาพที่ 25 ระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส จะทำการเรียกใช้การตรวจสอบข้อมูลผู้ต้องห้ามเข้าสถานที่จากระบบเว็บเซอร์วิสของสำนักงานความมั่นคงแห่งชาติ โดยการนำหมายเลขบัตรประจำตัวประชาชนของผู้ติดต่อขอเข้าสถานที่ไปตรวจสอบถ้าข้อมูลตรงจะได้ค่า “Y” ซึ่งหมายถึงผู้ติดต่อขอเข้าสถานที่เป็นบุคคลต้องห้าม จะไม่อนุญาตให้เข้าสถานที่ ในทางตรงกันข้ามถ้าได้ค่า “N” คือไม่มีการตรวจพบในฐานข้อมูลผู้ต้องห้ามเข้าสถานที่ จะให้ทำการตรวจสอบไปยังระบบเว็บเซอร์วิสสำนักงานตำรวจแห่งชาติต่อไป โดยรูปแบบการตอบกลับข้อมูลการตรวจสอบโดยแสดงเป็นโครงสร้างเอกสาร XML ดัง ภาพที่ 26



ภาพที่ 26 แสดงโครงสร้างเอกสาร XML ของเซอร์วิส fileblaclist

3. ระบบเว็บเซอร์วิสสำนักงานตำรวจแห่งชาติเปิดให้บริการ การตรวจสอบข้อมูลผู้ต้องห้าม

เว็บเซอร์วิสของระบบสำนักงานตำรวจแห่งชาติเปิดให้บริการดังนี้

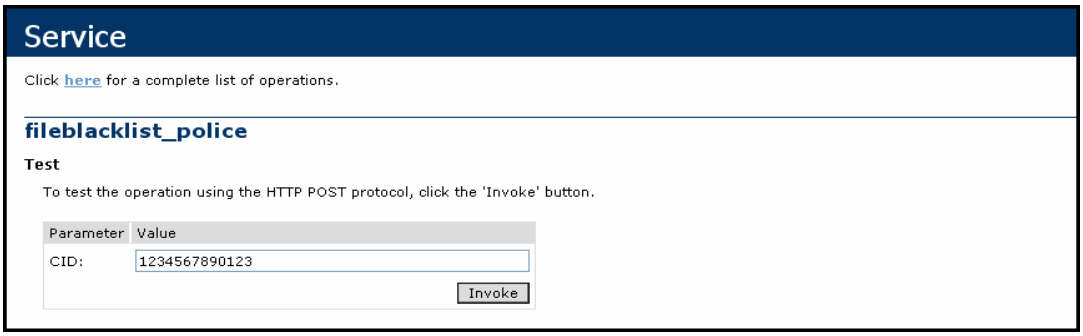
เซอร์วิสการตรวจสอบข้อมูลผู้ต้องห้ามเข้าสถานที่

ส่วนที่เปิดให้บริการ : สำนักงานตำรวจแห่งชาติ

ชื่อเซอร์วิส : fileblacklist_police

ข้อมูลที่รับเข้า : CID (หมายเลขบัตรประจำตัวประชาชน)

ผลที่ได้ : เป็นค่าของการตรวจสอบ “Y” คือค่าที่ตรวจสอบพบในฐานข้อมูล
“N” คือค่าที่ไม่มีการตรวจพบในฐานข้อมูล



ภาพที่ 27 แสดงเซอร์วิส fileblacklist_police

จากภาพที่ 27 ระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส จะทำการเรียกใช้การตรวจสอบข้อมูลผู้ต้องห้ามเข้าสถานที่จากระบบเว็บเซอร์วิสของสำนักงานตำรวจแห่งชาติอีกครั้ง หากการตรวจสอบข้อมูลจากระบบเว็บเซอร์วิสสำนักงานความมั่นคงแห่งชาติได้ค่า “N” โดยการนำหมายเลขบัตรประจำตัวประชาชนของผู้ติดต่อขอเข้าสถานที่ไปตรวจสอบถ้าข้อมูลตรงจะได้ค่า “Y” ซึ่งหมายความผู้ติดต่อขอเข้าสถานที่เป็นบุคคลต้องห้าม จะไม่อนุญาตให้เข้าสถานที่ ในทางตรงกันข้ามถ้าได้ค่า “N” คือไม่มีการตรวจพบในฐานข้อมูลผู้ต้องห้ามเข้าสถานที่ก็อนุญาตให้เข้าสถานที่ได้ โดยรูปแบบการตอบกลับข้อมูลการตรวจสอบโดยแสดงเป็นโครงสร้างเอกสาร XML ดัง ภาพที่ 28

```
<?xml version="1.0" encoding="utf-8" ?>
<string xmlns="http://tempuri.org/">Y</string>
```

ภาพที่ 28 แสดงโครงสร้างเอกสาร XML ของเซอร์วิส fileblaclist_police

ประเมินผลการทดสอบระบบ

1. การประเมินความพึงพอใจ

ผู้พัฒนาได้ทำการประเมินความพึงพอใจในการใช้งานระบบโดยวิธีการแจกแบบประเมินให้กับผู้ที่ทดลองใช้งานระบบได้แก่ เจ้าหน้าที่รักษาความปลอดภัยจำนวน 5 คน และเจ้าหน้าที่ด้านฝ่ายอาคารสถานที่จำนวน 6 คน จากโรงพยาบาลสัตว์ คณะสัตวแพทยศาสตร์ ม.เกษตรศาสตร์

บางเขน จังหวัด กรุงเทพมหานคร และ ศูนย์เทคโนโลยีชีวภาพเกษตร มหาวิทยาลัยเกษตรศาสตร์ วิทยาเขตกำแพงแสน โดยแบ่งการประเมินออกเป็นสองส่วนคือ

1.1 ประเมินความพึงพอใจในด้านการใช้งานระบบ

1.2 ประเมินความพึงพอใจในด้านการทำงานของระบบ

โดยหลักการให้คะแนนการประเมินเป็นดังนี้

มาก เท่ากับ 5 คะแนน

ดี เท่ากับ 4 คะแนน

พอใช้ เท่ากับ 3 คะแนน

ปรับปรุง เท่ากับ 2 คะแนน

ไม่เหมาะสม เท่ากับ 1 คะแนน

ตารางที่ 8 ตารางผลการประเมินความพึงพอใจด้านการใช้งานของเจ้าหน้าที่รักษาความปลอดภัย

รายละเอียดตาราง : ผลการประเมินความพึงพอใจด้านการใช้งานของระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส ของเจ้าหน้ารักษาความปลอดภัย					
รายการประเมิน	**เจ้าหน้ารักษาความปลอดภัย**				
	ระดับความคิดเห็น				
	มาก	**ดี**	**พอใช้**	**ปรับปรุง**	**ไม่เหมาะสม**
ขั้นตอนการทำงานเป็นระบบ ง่ายต่อการใช้งาน ไม่ซับซ้อน	0	3	2	0	0
ข้อมูลครบถ้วนตามความต้องการ	0	4	1	0	0
การประมวลผลจากระบบได้ผลลัพธ์ถูกต้องตามเหตุการณ์จริง	0	1	4	0	0
รูปแบบของหน้าจอสีตัวอักษรและรูปภาพที่ใช้ประกอบมีความเหมาะสม	0	2	3	0	0
เป็นประโยชน์ต่อการนำมาใช้ในระบบรักษาความปลอดภัย	0	3	2	0	0

ตารางที่ 9 ตารางผลการประเมินความพึงพอใจด้านการใช้งานของระบบของเจ้าหน้าที่ฝ่ายอาคารสถานที่

รายละเอียดตาราง : ผลการประเมินความพึงพอใจด้านการใช้งานของระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส ของเจ้าหน้าที่ฝ่ายอาคารสถานที่					
รายการประเมิน	**เจ้าหน้าที่ฝ่ายอาคารสถานที่**				
	ระดับความคิดเห็น				
	มาก	**ดี**	**พอใช้**	**ปรับปรุง**	**ไม่เหมาะสม**
ขั้นตอนการทำงานเป็นระบบ ง่ายต่อการใช้งานไม่ซับซ้อน	3	1	2	0	0
ข้อมูลครบถ้วนตามความต้องการ	0	4	2	0	0
การประมวลผลจากระบบได้ผลลัพธ์ถูกต้องตามเหตุการณ์จริง	0	3	3	0	0
รูปแบบของหน้าจอสีตัวอักษรและรูปภาพที่ใช้ประกอบมีความเหมาะสม	0	3	3	0	0
เป็นประโยชน์ต่อการนำมาใช้ในระบบรักษาความปลอดภัย	1	2	3	0	0

ตารางที่ 10 ตารางผลการประเมินความพึงพอใจด้านการทำงานของระบบของเจ้าหน้าที่รักษาความปลอดภัย

รายละเอียดตาราง : ผลการประเมินความพึงพอใจด้านการทำงานของระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส ของเจ้าหน้ารักษาความปลอดภัย					
รายการประเมิน	**เจ้าหน้าที่รักษาความปลอดภัย**				
	ระดับความคิดเห็น				
	มาก	**ดี**	**พอใช้**	**ปรับปรุง**	**ไม่เหมาะสม**
สะดวกรวดเร็วในการสืบค้นข้อมูล	0	2	3	0	0
ข้อมูลที่สืบค้นมีความถูกต้อง	1	2	2	0	0
ข้อมูลที่จัดเก็บมีความถูกต้อง	2	2	1	0	0
ความถูกต้องในการแก้ไขข้อมูล	2	2	1	0	0

ตารางที่ 10 (ต่อ)

รายละเอียดตาราง : ผลการประเมินความพึงพอใจด้านการทำงานของระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส ของเจ้าหน้ารักษาความปลอดภัย					
รายการประเมิน	**เจ้าหน้าที่รักษาความปลอดภัย**				
	ระดับความคิดเห็น				
	มาก	**ดี**	**พอใช้**	**ปรับปรุง**	**ไม่เหมาะสม**
ความเร็วในการประมวลผลข้อมูล	0	3	2	0	0
ความเร็วในการรับส่งข้อมูล	0	2	3	0	0

ตารางที่ 11 ผลการประเมินความพึงพอใจด้านการทำงานของระบบของเจ้าหน้าที่ฝ่ายอาคารสถานที่

รายละเอียดตาราง : ผลการประเมินความพึงพอใจด้านการทำงานของระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส ของเจ้าหน้าที่ฝ่ายอาคารสถานที่					
รายการประเมิน	**เจ้าหน้าที่ฝ่ายอาคารสถานที่**				
	ระดับความคิดเห็น				
	มาก	**ดี**	**พอใช้**	**ปรับปรุง**	**ไม่เหมาะสม**
สะดวกรวดเร็วในการสืบค้นข้อมูล	0	2	4	0	0
ข้อมูลที่สืบค้นมีความถูกต้อง	1	2	3	0	0
ข้อมูลที่จัดเก็บมีความถูกต้อง	1	2	3	0	0
ความถูกต้องในการแก้ไขข้อมูล	0	2	4	0	0
ความเร็วในการประมวลผลข้อมูล	0	4	2	0	0
ความเร็วในการรับส่งข้อมูล	0	3	3	0	0

ผลที่ได้จากการทำแบบประเมินความพึงพอใจจากการทดลองใช้งานระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส ผู้วิจัยได้นำผลมาวิเคราะห์โดยใช้ค่าเฉลี่ย ($\bar{X}$) ดังตาราง

ตารางที่ 12 ค่าเฉลี่ยของผลการประเมินความพึงพอใจในด้านการใช้งานระบบ

รายละเอียดตาราง : ค่าเฉลี่ยของผลการประเมินความพึงพอใจระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส ด้านการใช้งานระบบ		
รายการประเมิน	**ค่าเฉลี่ย ($\bar{X}$)**	**ระดับ**
1. ขั้นตอนการทำงานเป็นระบบ ง่ายต่อการใช้งานไม่ซับซ้อน	3.91	ดี
2. ข้อมูลครบถ้วนตามความต้องการ	3.73	ดี
3. การประมวลผลจากระบบได้ผลลัพธ์ถูก ต้องตามเหตุการณ์จริง	3.36	พอใช้
4. รูปแบบของหน้าจอสีตัวอักษรและรูปภาพที่ใช้ประกอบมีความเหมาะสม	3.45	พอใช้
5. เป็นประโยชน์ต่อการนำมาใช้ในระบบเวชระเบียน	3.64	ดี
รวมด้านการใช้งานระบบ	3.61	ดี

2. สรุปผลการวิเคราะห์

ผลการประเมินความพึงพอใจในด้านการใช้งานระบบผู้ใช้มีความพึงพอใจโดยมีค่าเฉลี่ยรวมเท่ากับ 3.61 อยู่ในระดับดี เนื่องจากระบบมีความสะดวกต่อการใช้งาน การประมวลผลลัพธ์ถูกต้อง รูปแบบหน้าจอมีความเหมาะสมและเป็นประโยชน์ต่อการนำมาใช้ในระบบรักษาความปลอดภัย

ตารางที่ 13 ค่าเฉลี่ยของผลการประเมินความพึงพอใจในด้านการทำงานของระบบ

รายละเอียดตาราง : ค่าเฉลี่ยของผลการประเมินความพึงพอใจระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส ด้านการทำงานของระบบ		
รายการประเมิน	**ค่าเฉลี่ย ($\bar{X}$)**	**ระดับ**
1. สะดวกรวดเร็วในการสืบค้นข้อมูล	3.36	พอใช้
2. ข้อมูลที่สืบค้นมีความถูกต้อง	3.73	ดี
3. ข้อมูลที่จัดเก็บมีความถูกต้อง	3.91	ดี
4. ความถูกต้องในการแก้ไขข้อมูล	3.73	ดี
5. ความเร็วในการประมวลผลข้อมูล	4.00	ดี
6. ความเร็วในการรับส่งข้อมูล	3.45	พอใช้
รวมด้านการทำงานของระบบ	3.69	ดี

ผลการประเมินความพึงพอใจในด้านการทำงานของระบบผู้ใช้มีความพึงพอใจโดยมีค่าเฉลี่ยรวมเท่ากับ 3.69 อยู่ในระดับดี เนื่องจากระบบมีความสะดวกรวดเร็วและถูกต้องในการสืบค้นข้อมูล จัดเก็บข้อมูล และการแก้ไขข้อมูล

บทที่ 5
บทสรุป

ระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส (Development of Access Control System using Web Service) ผู้วิจัยทำการศึกษา วิเคราะห์ ออกแบบ และพัฒนาระบบรักษาความปลอดภัยในการเข้า-ออกสถานที่ให้มีประสิทธิภาพมากขึ้นในด้านการรักษาความปลอดภัย โดยการนำอุปกรณ์และเครื่องมือที่เกี่ยวข้องในการพัฒนาดังนี้

1. บัตรประจำตัวประชาชนแบบสมาร์ตการ์ด ใช้ในการยืนยันตัวบุคคลว่าเป็นเจ้าของบัตรจริง โดยการสแกนลายนิ้วมือและเปรียบเทียบกับข้อมูลลายนิ้วมือในบัตร

2. กล้อง Web Cam เป็นอุปกรณ์ที่ใช้ในการจับภาพหน้าของผู้เข้าสถานที่ เพื่อให้ระบบมีความน่าเชื่อถือ และบันทึกลงฐานข้อมูลได้เพื่อใช้เป็นหลักฐานในการเข้า-ออกสถานที่ในแต่ละครั้งที่ทำการเข้าสถานที่

3. บริการเว็บเซอร์วิสโดยผู้วิจัยได้จำลองระบบเว็บเซอร์วิสทั้งหมด 3 ระบบ ได้แก่ ระบบสำนักงานทะเบียนราษฎร์มี Service showdetail ซึ่งทำหน้าที่ให้บริการข้อมูลประจำตัวประชาชนของผู้ติดต่อ ส่วนระบบเว็บเซอร์วิสสำนักงานตำรวจแห่งชาติมี Service fileblacklist และระบบเว็บเซอร์วิสสำนักงานความมั่นคงแห่งชาติมี Service fileblacklistโดยทั้ง 2 ระบบนี้จะทำหน้าที่ให้บริการข้อมูลผู้ต้องห้ามเข้าสถานที่ เพื่อใช้ในการตรวจสอบผู้ติดต่อ

สรุปผลการพัฒนาระบบการควบคุมการเข้า-ออกสถานที่โดยใช้เว็บเซอร์วิส

1. ผู้วิจัยได้นำเครื่องอ่านบัตรประชาชนแบบสมาร์ทการ์ดและพิสูจน์เอกลักษณ์ตัวบุคคลด้วยลายนิ้วมือ รุ่น IRIS XP-BIOCARDREADER เข้ามาทดสอบการอ่านข้อมูลในบัตรและการสแกนลายนิ้วมือว่าผู้ถือเป็นบัตรเจ้าของบัตรประจำตัวประชาชนจริงเพื่อป้องกันปลอมแปลงบัตรประจำตัวประชาชน ซึ่งจากการทดสอบระบบทำงานของเครื่อง IRIS XP-BIOCARDREADER สามารถใช้เปรียบเทียบลายนิ้วมือกับข้อมูลในบัตรประชาชนได้อย่างถูกต้อง

2. การบันทึกรูปหน้าผู้ติดต่อทุกครั้งที่มีการเข้าสถานที่ โดยการบันทึกรูปหน้าผู้ติดต่อนี้ระบบทำการจับภาพด้วยกล้อง Web Cam และทำการบันทึกลงฐานข้อมูลได้

3. การเรียกใช้ข้อมูลรูปหน้าผู้ติดต่อเข้าสถานที่ ทำได้โดยการค้นหาข้อมูลผู้ติดต่อที่ทำการเข้า-ออกสถานที่ ระบบจะแสดงรูปหน้าผู้ติดต่อด้วย

4. ผลการใช้บริการข้อมูลประจำตัวประชาชนของ Service showdetail จากระบบเว็บเซอร์วิสสำนักงานทะเบียนราษฎร์ ระบบได้รับข้อมูลที่ถูกต้องและครบถ้วน โดยข้อมูลที่ได้รับคือข้อมูลประจำตัวประชาชน และรูปใบหน้าของผู้ติดต่อ

5. ผลการใช้บริการข้อมูลการตรวจสอบผู้ต้องห้ามเข้าสถานที่ของ Service fileblacklist จากระบบสำนักงานความมั่นคงแห่งชาติ และ Service fileblacklist_police ของระบบเว็บเซอร์วิสสำนักงานตำรวจแห่งชาติ ระบบได้ผลการตรวจสอบที่ถูกต้องและแม่นยำ โดยข้อมูลที่ระบบได้รับกลับมาคือ “Y” ในกรณีผู้ติดต่อ มีข้อมูลตรงกับฐานข้อมูลผู้ต้องห้ามเข้าสถานที่ หรือ “N”ในกรณีผู้ติดต่อ มีข้อมูลไม่ตรงกับฐานข้อมูลผู้ต้องห้ามเข้า

สรุปผลประเมินระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส

ผลการประเมินหลังการทดลองใช้ระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส จำนวน 11 คน จากกลุ่มผู้ทดลองใช้ 2 กลุ่มคือ เจ้าหน้าที่ฝ่ายอาคารและสถานที่ และเจ้าหน้าที่รักษาความปลอดภัย จากโรงพยาบาลสัตว์ คณะสัตวแพทยศาสตร์ ม.เกษตรศาสตร์บางเขน จังหวัด กรุงเทพมหานคร และ ศูนย์เทคโนโลยีชีวภาพเกษตร มหาวิทยาลัยเกษตรศาสตร์ วิทยาเขตกำแพงแสน พบว่า ในด้านการใช้งานระบบผู้ทดสอบระบบมีความพึงพอใจโดยมีค่าเฉลี่ยรวม เท่ากับ 3.61 อยู่ในระดับดี เนื่องจากระบบมีความสะดวกและใช้งานง่าย การประมวลผลลัพธ์ถูกต้อง รูปแบบหน้าจอมีความเหมาะสมและเป็นประโยชน์กับระบบการรักษาความปลอดภัย ส่วนในด้านการทำงานของระบบผู้ทดสอบระบบมีความพึงพอใจโดยมีค่าเฉลี่ยรวม เท่ากับ 3.69 อยู่ในระดับดี เนื่องจากระบบมีความสะดวกรวดเร็วและถูกต้องในการสืบค้นข้อมูล จัดเก็บข้อมูล และการแก้ไขข้อมูล ผู้ทดลองระบบเห็นว่าระบบสามารถค้นหาข้อมูลได้รวดเร็วและถูกต้อง สามารถนำมาใช้กับระบบรักษาความปลอดภัยได้จริง

ข้อจำกัดของการศึกษา

1. ระบบเว็บเซอร์วิสที่ให้บริการข้อมูล ได้แก่ ระบบเว็บเซอร์วิสสำนักงานทะเบียนราษฎร์ ระบบเว็บเซอร์วิสสำนักงานความมั่นคงแห่งชาติ ระบบเว็บเซอร์วิสสำนักงานตำรวจแห่งชาติ เป็นระบบเว็บเซอร์วิสที่ผู้พัฒนาได้จำลองขึ้น เพื่อพัฒนาระบบ

2. ระบบนี้จะมุ้งเน้นการทำงานไปที่ผู้ที่มีบัตรประจำตัวประชาชนแบบสมาร์ทการ์ดเท่านั้น

ข้อเสนอแนะ

1. ในการแลกเปลี่ยนข้อมูลผ่านเว็บเซอร์วิสควรมีการรักษาความปลอดภัยของข้อมูลโดยการเข้ารหัสข้อมูลเพื่อความปลอดภัยของผู้ใช้บัตร

2. ในระบบควรการแจ้งเตือนไปยังสถานีตำรวจหรือหน่วยรักษาความปลอดภัยโดยอัตโนมัติหากพบผู้ต้องห้ามเข้าสถานที่ ทำการติดต่อขอเข้าสถานที่

3. ระบบควรที่จะแสดงรายงานได้ว่าบุคคลใดยังไม่ได้ออกจากสถานที่

4. ระบบควรเข้ารหัสข้อมูล Log file และ ข้อมูล Blacklist เพื่อป้องกันการเปลี่ยนแปลงหรือแก้ จากผู้ไม่ประสงค์ดี

5. ระบบควรค้นหาข้อมูลผู้เข้า-ออก สถานที่ โดยหาจาก ชื่อ หรือ นามสกุล ได้

บรรณานุกรม

ภาษาไทย

กษิร์พันธ์ มาสกุล. ไบโอเมทริก(Biometrics) [ออนไลน์]. เข้าถึงเมื่อ 6 พฤษภาคม 2550. ได้จาก http://www.spu.ac.th/~bmetric/fp_intro.htm

ณัฏฐ์นรี สุขจิต. "การพัฒนาต้นแบบสำหรับการท่องเที่ยวโดยใช้เทคโนโลยีเว็บเซอร์วิส." การค้นคว้าอิสระปริญญาวิทยาศาสตรมหาบัณฑิต คณะวิทยาศาสตร์ มหาวิทยาลัยอุบลราชธานี, 2549.

ปรัชญา พันธุ์มี และ ดวงแก้ว สวามิภักดิ์. การพิสูจน์ตัวตนในระบบเว็บเซอร์วิสด้วยระบบเคอร์เบอรอส (Web Services Authentication with The Kerberos System) [ออนไลน์]. เข้าถึงเมื่อ 3 สิงหาคม 2547. ได้จาก http://www.cs.tu.ac.th/tucs/th/abstract.html/T47_13_2547.pdf

วิศิษฎ์ นวอิทธิพร, สมพล แซ่ปึง และสิริวรรณ พรกิตติวัฒนากุล. "เว็บเซอร์วิสเชิงพื้นที่สำหรับระบบสารสนเทศภูมิศาสตร์." ปริญญานิพนธ์ปริญญาวิศวกรรมศาสตร์บัณฑิต ภาควิชาวิศวกรรมคอมพิวเตอร์ สถานบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, 2547.

สราวุธ อ้อยศรีสกุล และ วิทยา ต่อศรีเจริญ. ถอดรหัส .NET + Web Services. กรุงเทพฯ : บริษัทวิตตี้ กรุ๊ป จำกัด, 2544.

สุจิตรา อดุลย์เกษม และคนอื่น ๆ. "การควบคุมเข้าใช้งานระบบโดยพิสูจน์ลายพิมพ์ลายนิ้วมือ." วารสารเทคโนโลยีสารสนเทศ 3, 5 (มกราคม-มิถุนายน2550) : 24-28.

สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการสถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์/TU-RAC. การคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในบัตรประจำตัวแบบอเนกประสงค์(Smart Card). ม.ป.ท. , 2547.

HPCC Wiki. เอกสารเรื่องเว็บเซอร์วิสคืออะไร [ออนไลน์]. เข้าถึงเมื่อ 20 ธันวาคม 2549. ได้จาก http://mike.cpe.ku.ac.th/~ekkasit/files/tutorials/SOA-www.hpcc.nectec.or.th.doc

ภาษาต่างประเทศ

Best, John W. Research in Education**.** Englewood Cliffs, New Jersey : Pretice-Hall, Inc. 1970.

Fensel, D. and C. Bussler. The Web Service Modeling Framework WSMF. Vrije Universiteit Amsterdam (VU) And Oracle Corporation [Online]. Accessed 22 August 2005. Available from http://www.wsmo.org/papers/publications/wsmf.paper.pdf

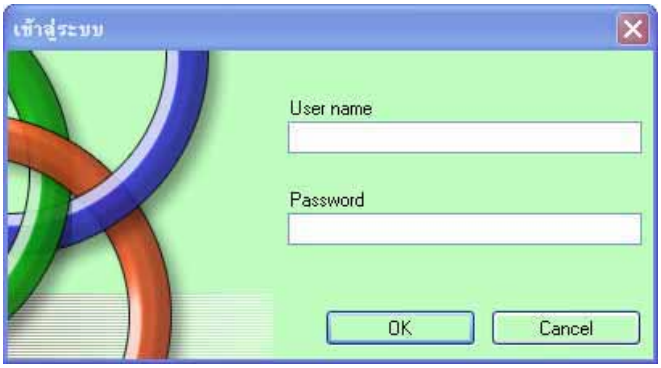
ภาคผนวก

ภาคผนวก ก
คู่มือการใช้งานโปรแกรม

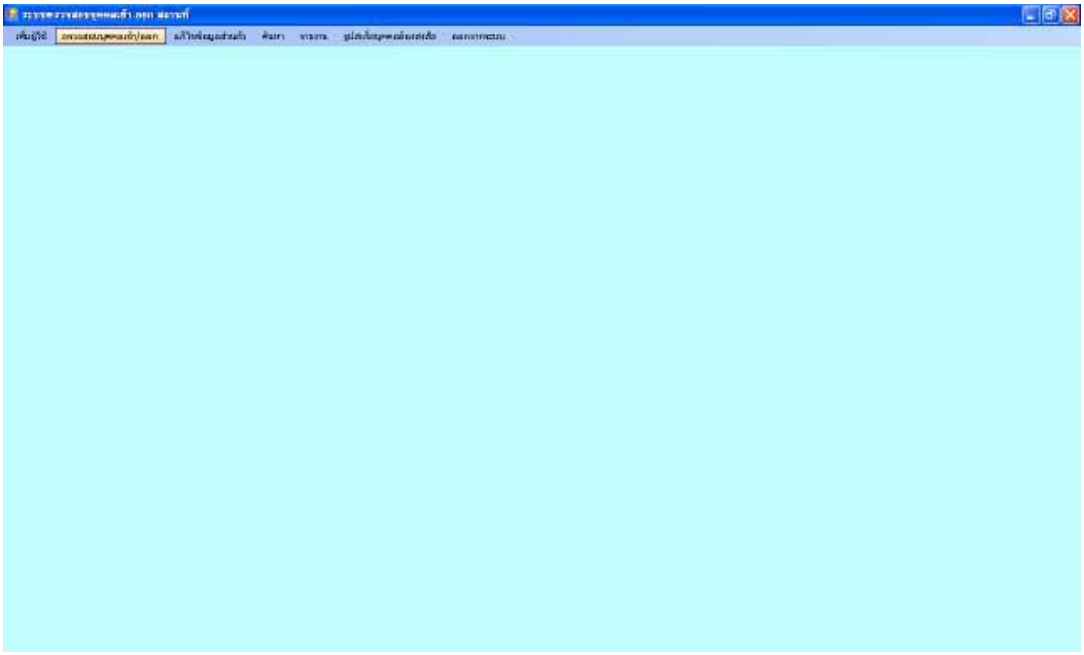
คู่มือการใช้โปรแกรม

คู่มือการใช้งานโปรแกรมนี้ จัดทำขึ้นเพื่อให้ผู้ใช้งานเข้าใจการทำงานของโปรแกรมและใช้โปรแกรมอย่างถูกต้อง ซึ่งโปรแกรมที่พัฒนาขึ้น เป็นโปรแกรมที่ใช้งานง่าย ในคู่มือการใช้โปรแกรมจะกล่าวเป็นขั้นตอนดังนี้

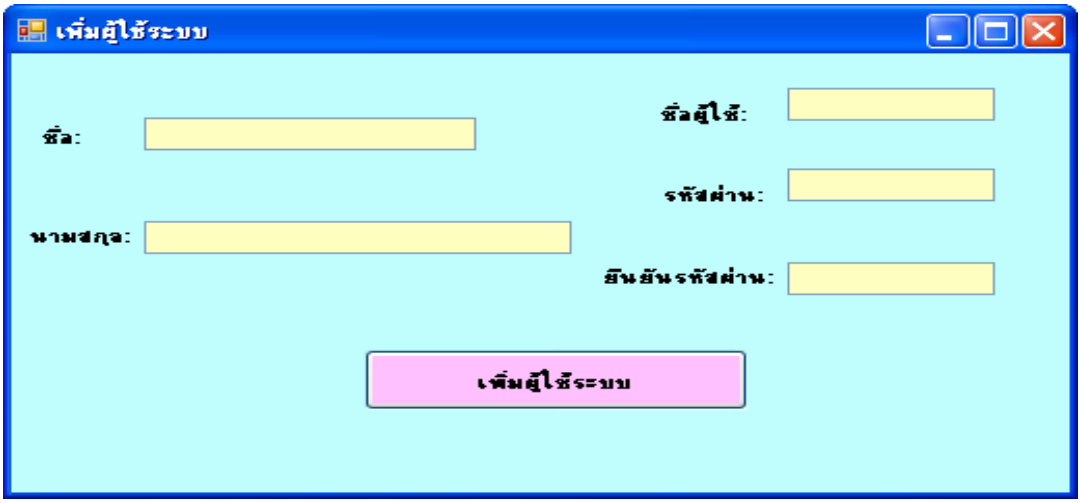
1. การเข้าใช้ระบบ ต้องใส่ชื่อผู้ใช้และรหัสในหน้าจอด้านล่าง



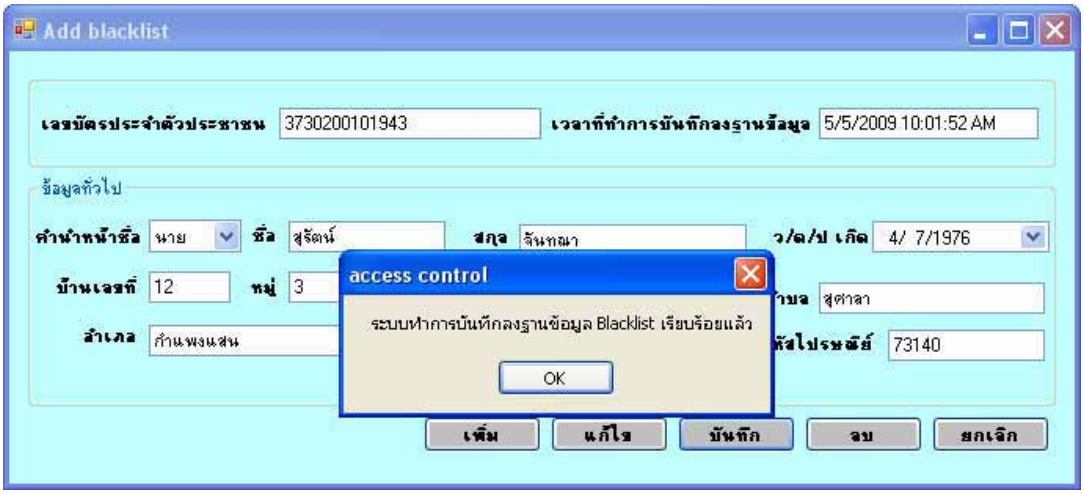
2. หลังจาก login เข้าระบบจะแสดงหน้าหลักการใช้งานโปรแกรมดังภาพด่านล่าง



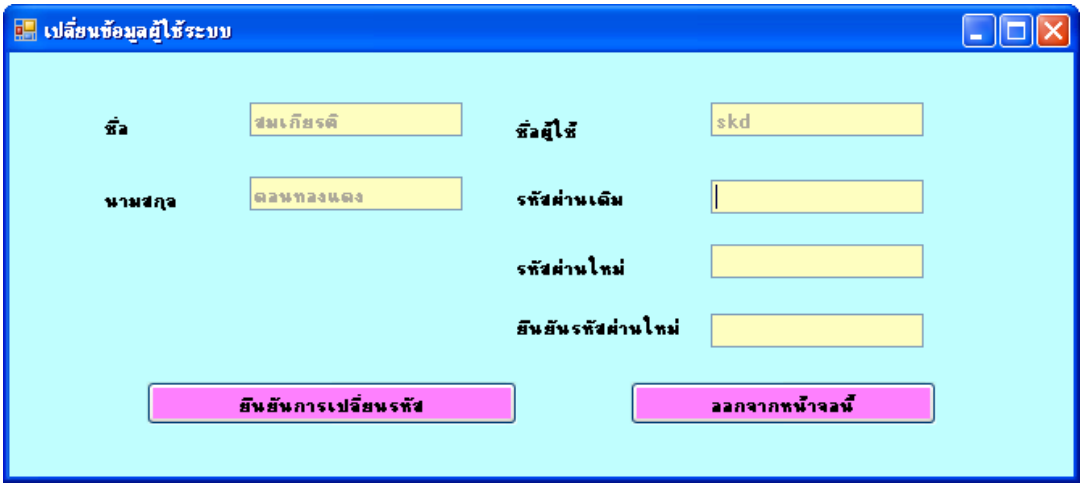
3. หน้าจอการเพิ่มผู้ใช้ระบบ เลือกจาก เมนูเพิ่มผู้ใช้จากหน้าจอหลัก การเพิ่มผู้ใช้ในระบบจะใช้ได้เฉพาะผู้ใช้ระบบที่มีสถานะเป็น Admin เท่านั้น



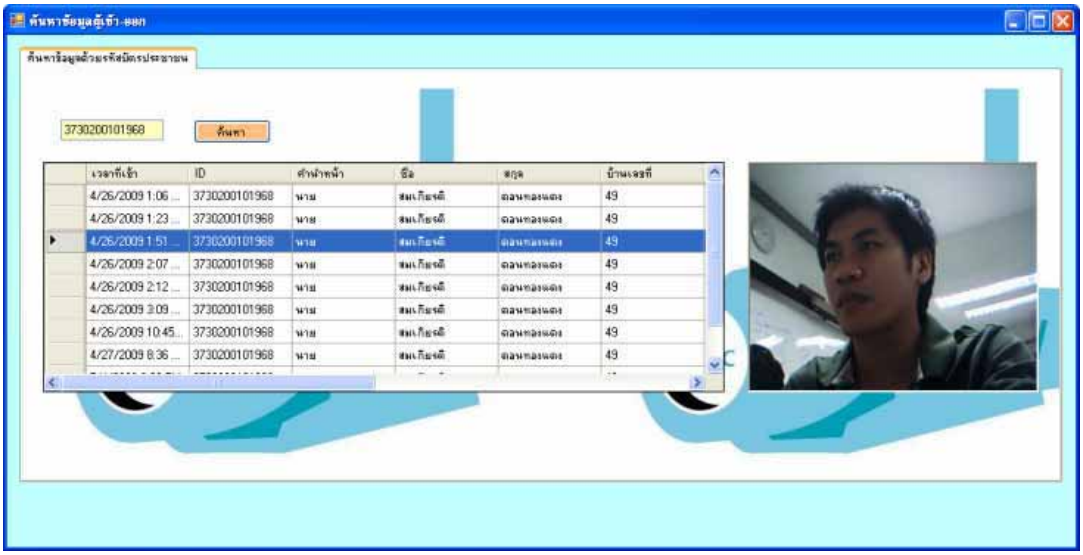
4. หน้าจอการเพิ่มข้อมูล Blacklist เลือกจาก เมนูเพิ่มข้อมูล เพิ่มข้อมูล Blacklist จากหน้าจอหลัก การเพิ่มข้อมูล Blacklist จะใช้ได้เฉพาะผู้ใช้ระบบที่มีสถานะเป็น Admin เท่านั้น



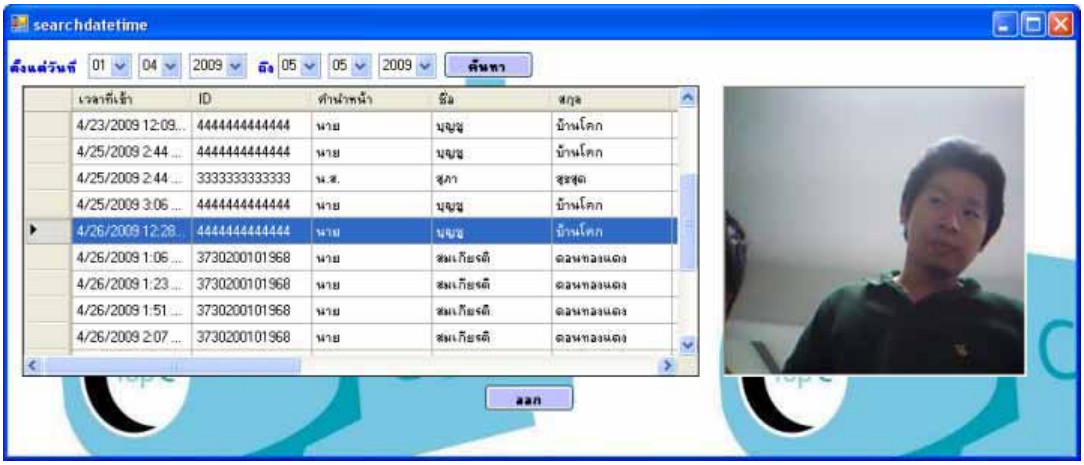
5. หน้าจอการเปลี่ยนข้อมูลผู้ใช้ระบบ เลือกจาก เมนูเพิ่มผู้ใช้จากหน้าจอหลัก โดยระบบจะจำข้อมูลส่วนตัวของผู้ใช้เมื่อทำการ login เข้าระบบ ดังภาพ



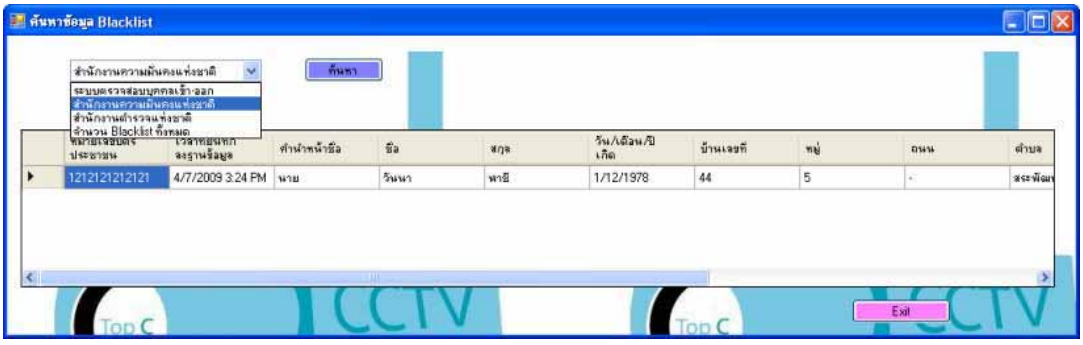
6. หน้าจอค้นหาข้อมูลเข้า-ออกสถานที่ตามรหัสบัตรประจำตัวประชาชน เลือกจากเมนูค้นหา ตามรหัสบัตรประชาชน จากหน้าจอหลัก แสดงดังภาพ



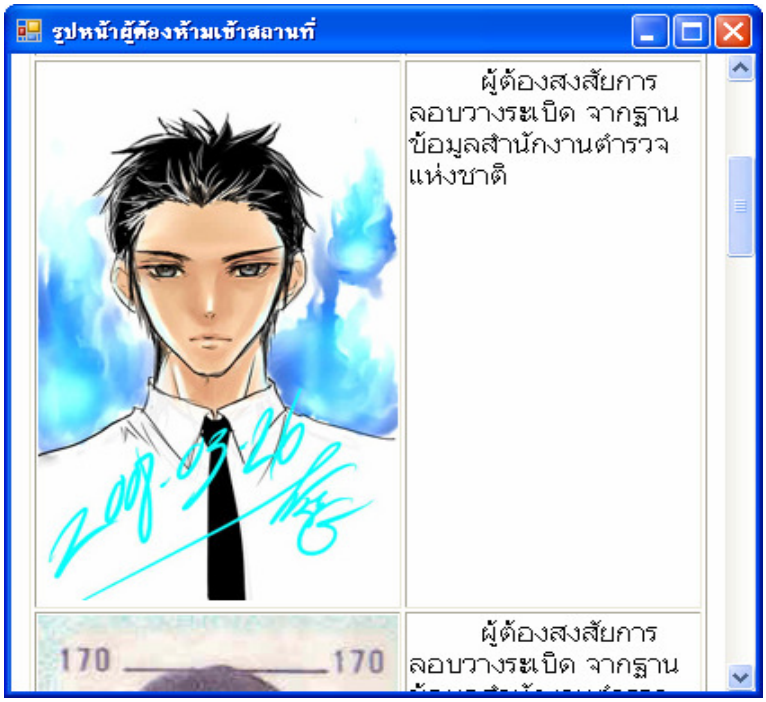
7. หน้าจอค้นหาข้อมูลเข้า-ออกสถานที่ตามช่วงเวลา เลือกจากเมนูค้นหา ตามวันเวลาการเข้าสถานที่จากหน้าจอหลัก แสดงหน้าจอดังภาพ



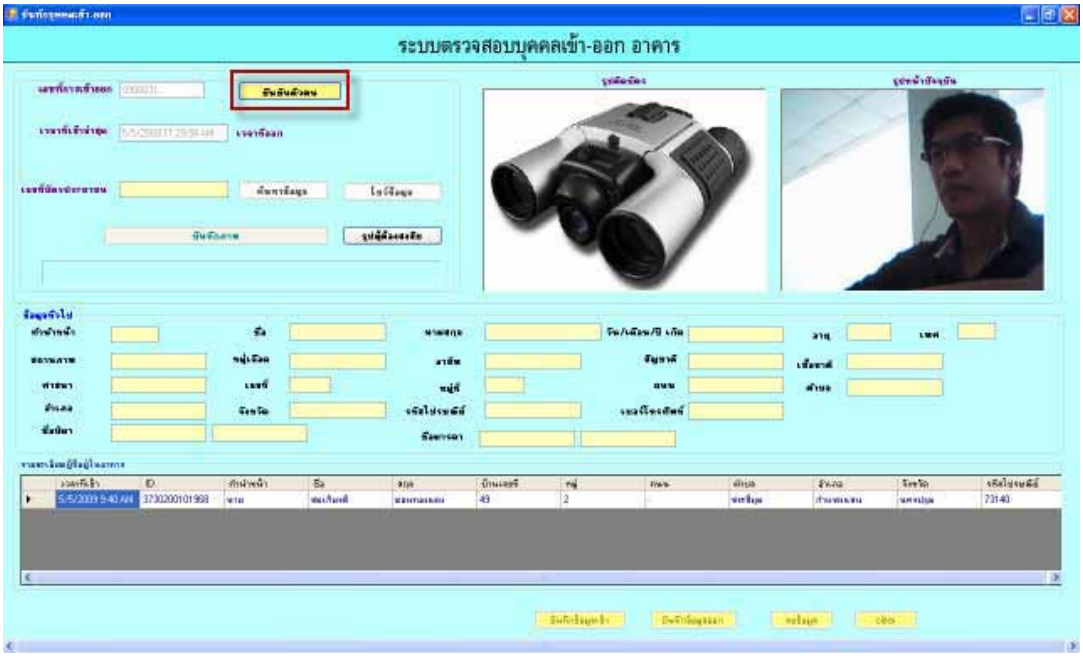
8. หน้าจอค้นหาข้อมูล Blacklist สามารถเลือกได้ว่าต้องข้อมูลจากฐานข้อมูลใด จากเมนูค้นหา ข้อมูล Blacklist ให้หน้าจอหลัก แสดงหน้าจอดังภาพ



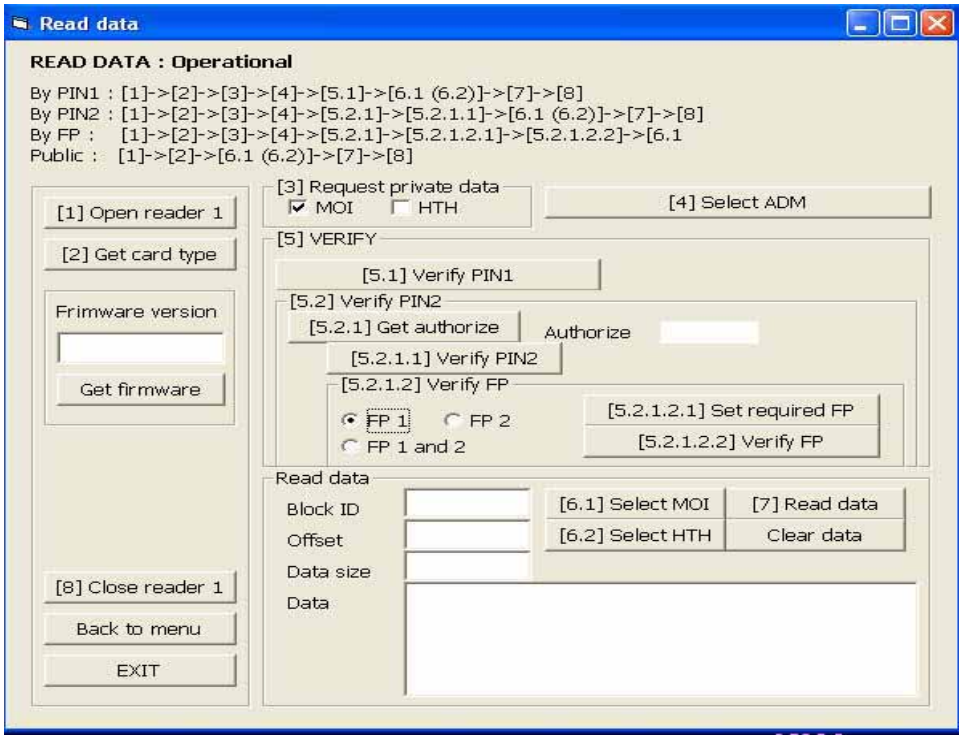
9. หน้าจอรูปบุคคลต้องสงสัย เลือกเมนูรูปผู้ต้องสงสัย ในหน้าจอหลักจะปรากฏหน้าจอดังภาพ



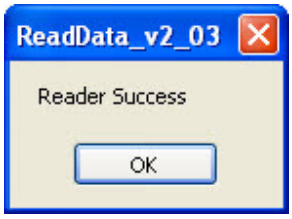
10. หน้าจอระบบการตรวจสอบบุคคลเข้า-ออกสถานที่ ต้องทำยืนยันตัวตนโดยการสแกนลายนิ้วมือ เพื่อยืนยันความเป็นเจ้าของบัตร โดยเลือกปุ่มยืนยันบุคคล



11. เข้าหน้าจอการยืนยันตัวบุคคลด้วยลายนิ้วมือกดปุ่ม Authentication แสดงหน้าจอการยืนยันตัวบุคคล ดังภาพ

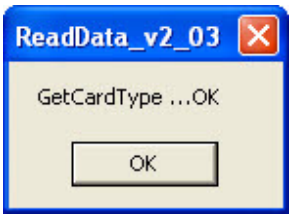


12. เลือก [1] open reader 1 จากหน้าจอ Read data เพื่อแสดงระบบสถานะพร้อมการใช้งานแสดงข้อความ ดังภาพ



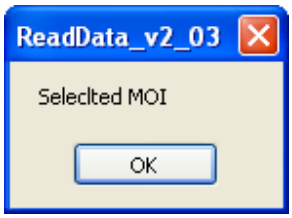
13. ใส่บัตรประชาชนแบบสมาร์ทการ์ดในเครื่องอ่านบัตรประชาชนแบบสมาร์ทการ์ดและพิสูจน์เอกลักษณ์ตัวบุคคลด้วยลายนิ้วมือ รุ่น IRIS XP-BIOCARDREADER

14. เลือก [2] Get card type จากหน้าจอ Read data เพื่อเลือกใช้การอ่านข้อมูลจากบัตรประชาชนแบบสมาร์ทการ์ดจะแสดงข้อความ ดังภาพ

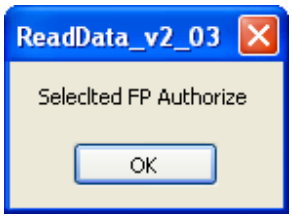


15. เลือก MOI ใน [3] Request Private data จากหน้าจอ Read data เพื่อเป็นการเลือกใช้ข้อมูลจากฐานข้อมูลกรมการปกครอง

16. เลือกปุ่ม Select AMD จากหน้าจอ Read data เพื่อยืนยันการใช้ฐานข้อมูลของกรมการปกครอง จะแสดงข้อความ ดังภาพ



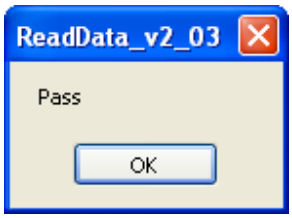
17. เลือกปุ่ม [5.2.1] Get Authorize จากหน้าจอ Read data เพื่อใช้การยืนยันตัวตนโดยการสแกนลายนิ้วมือจะแสดงข้อความ ดังภาพ



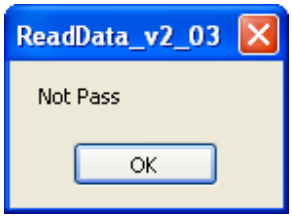
18. เลือก FP1 แล้วเลือกปุ่ม [5.2.1.2.1] Set Required FP เพื่อเป็นการเลือกสแกนนิ้วชี้ด้านซ้าย หรือเลือก FP2 เพื่อเป็นการเลือกสแกนนิ้วชี้ด้านขวา หรือ เลือก FP1 AND 2 เพื่อเป็นการเลือกสแกนนิ้วชี้ด้านซ้ายและขวา แล้วเลือกปุ่ม [5.2.1.2.1] Set Required FP เพื่อเป็นการยืนยันการเลือกใช้นิ้วในการสแกน

19. เลือกปุ่ม [5.2.1.2.2] Verify FP จะแจ้งข้อความให้วางนิ้วที่เลือกในการสแกนบนเครื่องอ่านบัตรประชาชนแบบสมาร์ทการ์ดและพิสูจน์เอกลักษณ์ตัวบุคคลด้วยลายนิ้วมือ รุ่น IRIS XP-BIOCARDREADERจะแสดงข้อความ ดังภาพ

20. เลือกปุ่ม OK จากข้อ 9 ถ้าลายนิ้วมือผู้ถือบัตรตรงกับข้อมูลลายนิ้วมือในบัตรจะปรากฏข้อความ ดังภาพแสดงลายนิ้วมือผู้ถือบัตรตรงกับข้อมูลลายนิ้วมือในบัตรถ้าลายนิ้วมือผู้ถือบัตรไม่ตรงกับข้อมูลลายนิ้วมือในบัตรจะขึ้นข้อความดังภาพภาพแสดงลายนิ้วมือผู้ถือบัตรไม่ตรงกับข้อมูลลายนิ้วมือในบัตร

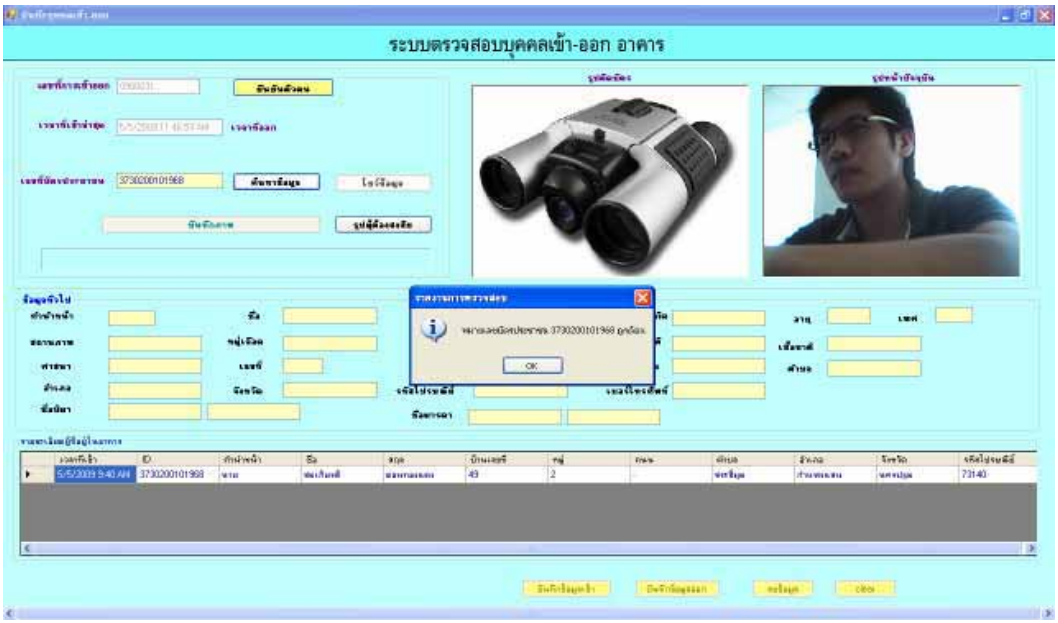


ภาพแสดงลายนิ้วมือผู้ถือบัตรตรงกับข้อมูลลายนิ้วมือในบัตร



ภาพแสดงลายนิ้วมือผู้ถือบัตรไม่ตรงกับข้อมูลลายนิ้วมือในบัตร

21. หลังจากขั้นตอนการยืนยันตัวบุคคลเรียบร้อยระบบจะได้รับ รหัสประจำตัวประชาชน 13 หลัก แล้วเลือกปุ่ม ค้นหาข้อมูลระบบจะมีการตรวจสอบอีกครั้งว่าหมายบัตรถูกต้องหรือไม่ ดังภาพ

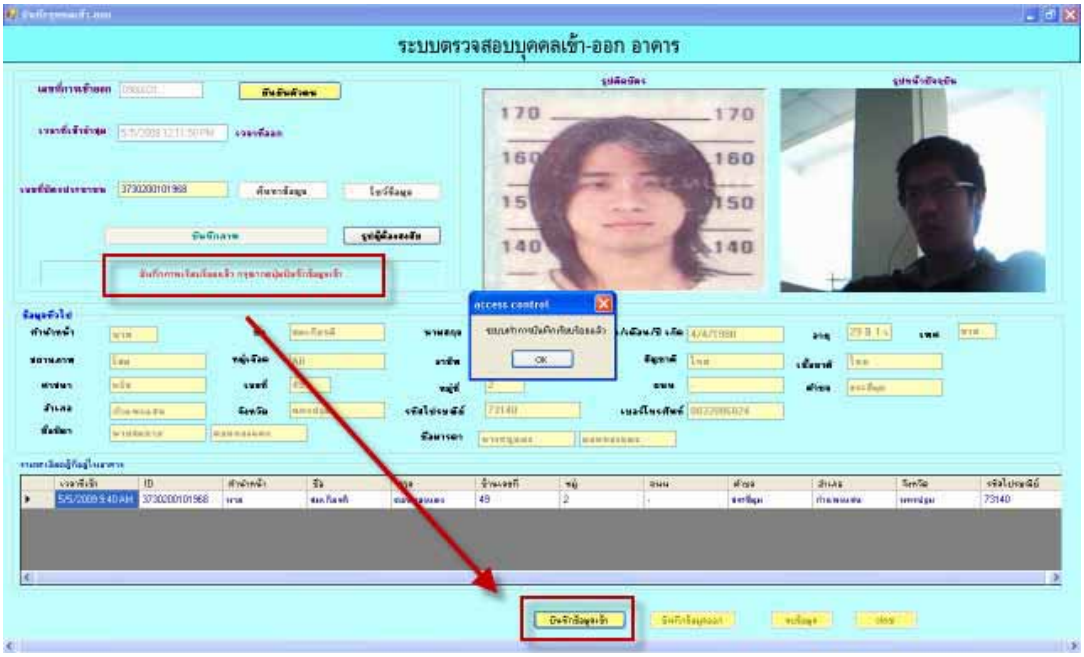


22. ระบบทำการใช้บริการข้อมูลของระบบเว็บเซอร์วิสสำนักงานทะเบียนราษฎร์ ที่ให้บริการข้อมูลประจำตัวประชาชนเพื่อนำมาแสดงผล จากนั้นระบบจะทำการตรวจสอบข้อมูลผู้เข้าสถานที่ ว่าตรงกับฐานข้อมูล Blacklist ของฐานข้อมูลระบบการตรวจสอบบุคคลเข้า- ออกสถานที่ฐานข้อมูลสำนักงานความมั่นคงแห่งชาติ และสำนักงานตำรวจแห่งชาติหรือไม่ ถ้าไม่ตรงจะแสดงข้อความดังภาพ ในหน้าจอนี้เจ้าหน้าที่ต้องใช้สายตาในการเปรียบเทียบรูปติดบัตรกับรูปปัจจุบันด้วยว่าเป็นคนคนเดียวกันหรือไม่

23. หากเปรียบเทียบรูปติดบัตรกับรูปปัจจุบันด้วยแล้วไม่เป็นคนคนเดียวกันให้เจ้าหน้าที่เลือกปุ่ม รูปผู้ต้องสงสัยเพื่อทำการเปรียบเทียบว่าเหมือนกันหรือไม่ ดังภาพ

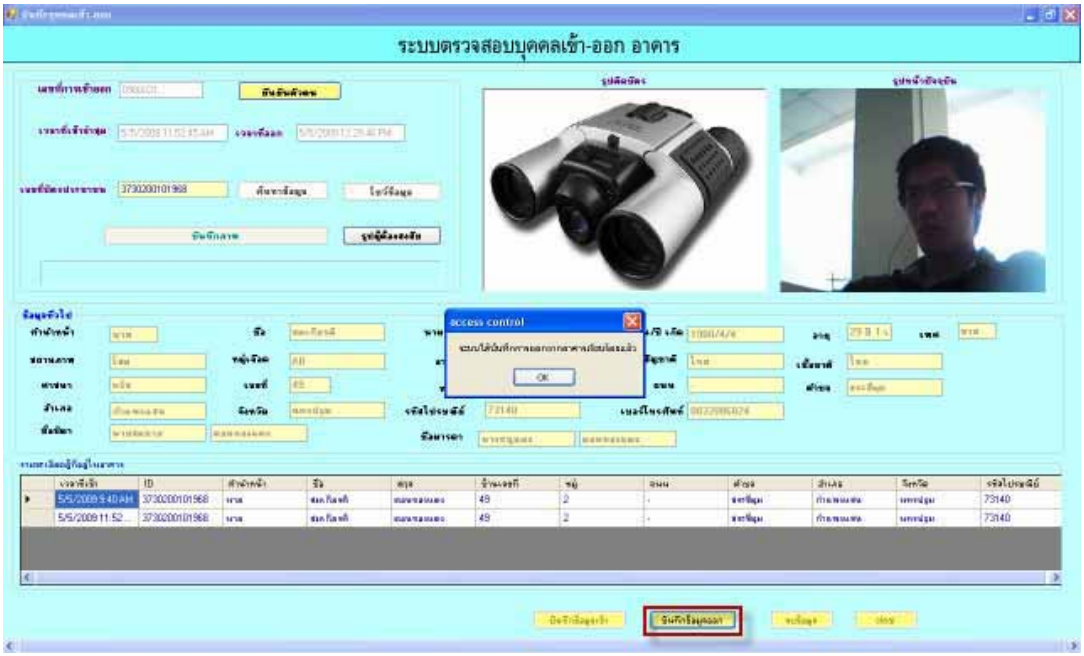
24. หากไม่มีปัญหาใด จะทำการบันทึกรูปหน้าผู้เข้าสถานที่และมีข้อความแจ้งชื่อของรูปภาพที่ทำการบันทึก ดังภาพ

25. หลังจากบันทึกรูปหน้าผู้เข้าสถานที่แล้ว ระบบจะแสดงข้อความ บันทึกภาพเรียบร้อยแล้ว กรุณากดปุ่มบันทึกข้อมูล เพื่อทำการบันทึกข้อมูล ดังภาพ



26. ขั้นตอนการบันทึกเวลาการออกสถานที่ เลือกข้อมูลผู้ที่ยังอยู่ในสถานที่จะแสดงใน Datagrid (ลูกศรชี้) และเลือกปุ่มโชว์ข้อมูล ดังภาพ

27. เลือกปุ่มบันทึกข้อมูลระบบจะแสดงข้อความการบันทึกข้อมูลออกจากสถานที่เรียบร้อยแล้ว ดังภาพ



ภาคผนวก ข

แบบประเมินผลการทดสอบระบบ

แบบประเมินผลการทดสอบระบบ

ผู้พัฒนาได้ทำการประเมินความพึ่งพอใจในการใช้งานระบบโดยวิธีการแจกแบบประเมินให้กับผู้ที่ทดลองใช้งานระบบได้แก่ เจ้าหน้าที่รักษาความปลอดภัยจำนวน 5 คน และเจ้าหน้าที่ด้านฝ่ายอาคารสถานที่จำนวน 6 คน จากโรงพยาบาลสัตว์ คณะสัตวแพทยศาสตร์ ม.เกษตรศาสตร์บางเขน จังหวัด กรุงเทพมหานคร และศูนย์เทคโนโลยีชีวภาพเกษตร มหาวิทยาลัยเกษตรศาสตร์ วิทยาเขตกำแพงแสน โดยแบ่งการประเมินออกเป็น 2 ส่วนคือ

1. ประเมินความพึงพอใจในด้านการใช้งานระบบ

ผลการประเมินความพึงพอใจด้านการใช้งานของเจ้าหน้ารักษาความปลอดภัย					
รายละเอียดตาราง : ผลการประเมินความพึงพอใจด้านการใช้งานของระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส ของเจ้าหน้ารักษาความปลอดภัย					
รายการประเมิน	**เจ้าหน้ารักษาความปลอดภัย**				
	ระดับความคิดเห็น				
	มาก	**ดี**	**พอใช้**	**ปรับปรุง**	**ไม่เหมาะสม**
ขั้นตอนการทำงานเป็นระบบ ง่ายต่อการใช้งานไม่ซับซ้อน					
ข้อมูลครบถ้วนตามความต้องการ					
การประมวลผลจากระบบได้ผลลัพธ์ถูก ต้องตามเหตุการณ์จริง					
รูปแบบของหน้าจอสีตัวอักษรและรูปภาพที่ใช้ประกอบมีความเหมาะสม					
เป็นประโยชน์ต่อการนำมาใช้ในระบบรักษาความปลอดภัย					

ผลการประเมินความพึงพอใจด้านการใช้งานของระบบของเจ้าหน้าที่ฝ่ายอาคารสถานที่					
รายละเอียดตาราง : ผลการประเมินความพึงพอใจด้านการใช้งานของระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส ของเจ้าหน้าที่ฝ่ายอาคารสถานที่					
รายการประเมิน	**เจ้าหน้าที่ฝ่ายอาคารสถานที่**				
	ระดับความคิดเห็น				
	มาก	**ดี**	**พอใช้**	**ปรับปรุง**	**ไม่เหมาะสม**
ขั้นตอนการทำงานเป็นระบบ ง่ายต่อการใช้งานไม่ซับซ้อน					
ข้อมูลครบถ้วนตามความต้องการ					
การประมวลผลจากระบบได้ผลลัพธ์ถูกต้องตามเหตุการณ์จริง					
รูปแบบของหน้าจอสีตัวอักษรและรูปภาพที่ใช้ประกอบมีความเหมาะสม					
เป็นประโยชน์ต่อการนำมาใช้ในระบบรักษาความปลอดภัย					

2. ประเมินความพึงพอใจในด้านการทำงานของระบบ

ตารางผลการประเมินความพึงพอใจด้านการทำงานของระบบของเจ้าหน้าที่รักษาความปลอดภัย					
รายละเอียดตาราง : ผลการประเมินความพึงพอใจด้านการทำงานของระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส ของเจ้าหน้าที่รักษาความปลอดภัย					
รายการประเมิน	**เจ้าหน้าที่รักษาความปลอดภัย**				
	ระดับความคิดเห็น				
	มาก	**ดี**	**พอใช้**	**ปรับปรุง**	**ไม่เหมาะสม**
สะดวกรวดเร็วในการสืบค้นข้อมูล					
ข้อมูลที่สืบค้นมีความถูกต้อง					
ข้อมูลที่จัดเก็บมีความถูกต้อง					
ความถูกต้องในการแก้ไขข้อมูล					
ความเร็วในการประมวลผลข้อมูล					
ความเร็วในการรับส่งข้อมูล					

ผลการประเมินความพึงพอใจด้านการทำงานของระบบของเจ้าหน้าที่ฝ่ายอาคารสถานที่					
รายละเอียดตาราง : ผลการประเมินความพึงพอใจด้านการทำงานของระบบการควบคุมการเข้า-ออกสถานที่ โดยใช้เว็บเซอร์วิส ของเจ้าหน้าที่ฝ่ายอาคารสถานที่					
รายการประเมิน	**เจ้าหน้าที่ฝ่ายอาคารสถานที่**				
	ระดับความคิดเห็น				
	มาก	**ดี**	**พอใช้**	**ปรับปรุง**	**ไม่เหมาะสม**
สะดวกรวดเร็วในการสืบค้นข้อมูล					
ข้อมูลที่สืบค้นมีความถูกต้อง					
ข้อมูลที่จัดเก็บมีความถูกต้อง					
ความถูกต้องในการแก้ไขข้อมูล					
ความเร็วในการประมวลผลข้อมูล					
ความเร็วในการรับส่งข้อมูล					

ภาคผนวก ค
ตารางฐานข้อมูลระบบ

ตารางที่ 14 ตารางเจ้าหน้าที่

ชื่อตาราง: Staff						
รายละเอียดตาราง: เก็บรายละเอียดเจ้าหน้าที่						
ลำดับที่	**ชื่อรายการข้อมูล**	**ประเภท**	**ขนาด**	**คำอธิบาย**	**หมายเหตุ**	**ตารางอ้างอิง**
1	user_Id	Text	10	ชื่อผู้ใช้	PK	
2	pass	Text	10	รหัสผู้ใช้		
3	name	Text	15	ชื่อ		
4	sername	Text	30	นามสกุล		
5	Status_id	Text	2	รหัสสถานะผู้ใช้	FK	Admin

ตารางที่ 15 เก็บสถานะผู้ใช้

ชื่อตาราง: Admin						
รายละเอียดตาราง: เก็บรายละเอียดสถานะผู้ใช้ระบบ						
ลำดับที่	**ชื่อรายการข้อมูล**	**ประเภท**	**ขนาด**	**คำอธิบาย**	**หมายเหตุ**	**ตารางอ้างอิง**
1	Status_id	Text	2	รหัสสถานะ	PK	
2	Status_detail	Text	10	รายละเอียดสถานะ		

ตารางที่ 16 ที่มาข้อมูลผู้ต้องห้ามเข้าสถานที่

ชื่อตาราง: Blacklist_form_DB						
รายละเอียดตาราง: เก็บที่มาข้อมูลผู้ต้องห้ามเข้าสถานที่						
ลำดับที่	**ชื่อรายการข้อมูล**	**ประเภท**	**ขนาด**	**คำอธิบาย**	**หมายเหตุ**	**ตารางอ้างอิง**
1	B_form_DB_id	Text	20	รหัสที่มาข้อมูลBlacklist	PK	
2	B_form_DB_detail	Text	30	รายละเอียดที่มาข้อมูล		

ตารางที่ 17 ข้อมูลผู้ต้องห้ามเข้าสถานที่ ทำการขอเข้าสถานที่

ชื่อตาราง:Blacklist_Incom						
รายละเอียดตาราง: เก็บข้อมูลผู้ต้องห้ามเข้าสถานที่ ทำการขอเข้าสถานที่						
ลำดับที่	**ชื่อรายการข้อมูล**	**ประเภท**	**ขนาด**	**คำอธิบาย**	**หมายเหตุ**	**ตารางอ้างอิง**
1	blacklist_Id	Text	13	รหัส Blacklist	PK	
2	Pname_Id	Text	3	รหัสคำนำหน้าชื่อ	FK	pname
3	blacklist_Name	Text	30	ชื่อ		
4	blacklist_SName	Text	50	สกุล		
5	blacklist_Birthday	Date/Time		วันเดือนปี เกิด		
6	blacklist_Income	Date/Time		วันเวลาที่เข้าสถานที่		
7	blacklist_add_num	Text	10	บ้านเลขที่		
8	blacklist_add_mu	Text	3	หมู่ที่		
9	blacklist_add_road	Text	30	ถนน		
10	blacklist_add_tumbon	Text	30	ตำบล		
11	blacklist_add_aumper	Text	30	อำเภอ		
12	Province_Id[	Text	2	รหัสจังหวัด	FK	province
13	blacklist_zipcode	Text	5	รหัสไปรษณีย์		

ตารางที่ 18 ประเภทหมู่เลือด

ชื่อตาราง: bloodgroup						
รายละเอียดตาราง: เก็บรายละเอียดหมู่เลือด						
ลำดับที่	**ชื่อรายการข้อมูล**	**ประเภท**	**ขนาด**	**คำอธิบาย**	**หมายเหตุ**	**ตารางอ้างอิง**
1	blood_id	Text	2	รหัสหมู่เลือด	PK	
1	blood_detail	Text	2	รายละเอียดหมู่เลือด		

ตารางที่ 19 ประเภทสัญชาติ

ชื่อตาราง: citizenship						
รายละเอียดตาราง: เก็บรายละเอียดสัญชาติ						
ลำดับที่	**ชื่อรายการข้อมูล**	**ประเภท**	**ขนาด**	**คำอธิบาย**	**หมายเหตุ**	**ตารางอ้างอิง**
1	citizenship_id	Text	4	รหัสสัญชาติ	PK	
2	citizenship_detail	Text	15	รายละเอียดรหัสสัญชาติ		

ตารางที่ 20 ประเภทสถานภาพ

ชื่อตาราง: marital_status						
รายละเอียดตาราง: เก็บประเภทของสถานภาพ						
ลำดับที่	**ชื่อรายการข้อมูล**	**ประเภท**	**ขนาด**	**คำอธิบาย**	**หมายเหตุ**	**ตารางอ้างอิง**
1	marital_id	Text	2	รหัสสถานภาพ	PK	
2	marital_detail	Text	10	รายละเอียดสถานภาพ		

ตารางที่ 21 ประเภทอาชีพ

ชื่อตาราง: Occuption						
รายละเอียดตาราง: เก็บประเภทของอาชีพ						
ลำดับที่	**ชื่อรายการข้อมูล**	**ประเภท**	**ขนาด**	**คำอธิบาย**	**หมายเหตุ**	**ตารางอ้างอิง**
1	Occ_id	Text	3	รหัสอาชีพ	PK	
2	Occ_detail	Text	20	รายละเอียดอาชีพ		

ตารางที่ 22 คำนำหน้าชื่อ

ชื่อตาราง: pname						
รายละเอียดตาราง: เก็บคำนำหน้าชื่อ						
ลำดับที่	**ชื่อรายการข้อมูล**	**ประเภท**	**ขนาด**	**คำอธิบาย**	**หมายเหตุ**	**ตารางอ้างอิง**
1	pname_id	Text	3	รหัสคำนำหน้าชื่อ	PK	
2	pname_detail	Text	5	รายละเอียดคำนำหน้าชื่อ		

ตารางที่ 23 จังหวัด

ชื่อตาราง: province						
รายละเอียดตาราง: เก็บประเภทจังหวัด						
ลำดับที่	**ชื่อรายการข้อมูล**	**ประเภท**	**ขนาด**	**คำอธิบาย**	**หมายเหตุ**	**ตารางอ้างอิง**
1	province_id	Text	4	รหัสจังหวัด	PK	
2	province_detail	Text	20	รายละเอียดจังหวัด		

ตารางที่ 24 ศาสนา

ชื่อตาราง: religion						
รายละเอียดตาราง: เก็บประเภทของศาสนา						
ลำดับที่	**ชื่อรายการข้อมูล**	**ประเภท**	**ขนาด**	**คำอธิบาย**	**หมายเหตุ**	**ตารางอ้างอิง**
1	religion_id	Text	3	รหัสศาสนา	PK	
2	region_detail	Text	10	รายละเอียดรหัสศาสนา		

ตารางที่ 25 เพศ

ชื่อตาราง: sex						
รายละเอียดตาราง: เก็บประเภทของเพศ						
ลำดับที่	**ชื่อรายการข้อมูล**	**ประเภท**	**ขนาด**	**คำอธิบาย**	**หมายเหตุ**	**ตารางอ้างอิง**
1	sex_id	Text	2	รหัสเพศ	PK	
2	sex_detail	Text	4	รายละเอียดเพศ		

ตารางที่ 26 ข้อมูล Blacklist

ชื่อตาราง: blacklist						
รายละเอียดตาราง: เก็บข้อมูลผู้ต้องห้ามเข้าสถานที่						
ลำดับที่	**ชื่อรายการข้อมูล**	**ประเภท**	**ขนาด**	**คำอธิบาย**	**หมายเหตุ**	**ตารางอ้างอิง**
1	Blacklist_Id	Text	13	รหัส Blacklist	PK	
2	B_Income	Date/Time		เวลาที่ทำการบันทึก		
3	pname_id	Text	3	รหัสคำนำหน้าชื่อ	FK	pname
4	B_fname	Text	30	ชื่อ		
5	B_lname	Text	30	สกุล		
6	B_birthday	DateTime		วันเดือนปี เกิด		
7	B_addrpart	Text	9	บ้านเลขที่		
8	B_moopart	Text	3	หมู่ที่		
9	B_amppart	Text	30	อำเภอ		
10	B_tmbpart	Text	30	ตำบล		
11	B_road	Text	30	ถนน		
12	province_id	Text	4	รหัสจังหวัด	FK	province
13	B_po_code	Text	7	รหัสไปรษณีย์		
14	B_form_DB_id	Text	2	รหัสที่มาข้อมูล Blacklist	FK	Blacklist_form_DB

ตารางที่ 27 ข้อมูลผู้เข้า-ออกสถานที่

ชื่อตาราง: visitor						
รายละเอียดตาราง: เก็บข้อมูลผู้เข้า-ออกสถานที่						
ลำดับที่	**ชื่อรายการข้อมูล**	**ประเภท**	**ขนาด**	**คำอธิบาย**	**หมายเหตุ**	**ตารางอ้างอิง**
1	cid	Text	13	รหัสบัตรประชาชน	PK	
2	Visitor_numb	Text	15	ลำดับการเข้าสถานที่	PK	
3	Time_in	Date/Time		เวลาเข้า		
4	pname_id	Text	3	รหัสคำนำหน้าชื่อ	FK	pname
5	fname	Text	30	ชื่อ		
6	lname	Text	30	สกุล		
7	birthday	Date/Time		วันเดือนปี เกิด		
8	citizenship_id	Text	4	รหัสสัญชาติ	FK	citizenship
9	nationality	Text	3	เชื้อชาติ		
10	Occ_id	Text	3	รหัสอาชีพ	FK	Occuption
11	blood_id	Text	2	รหัสหมู่เลือด	FK	bloodgroup
12	religion_id	Text	3	รหัสศาสนา	FK	religion
13	addrpart	Text	9	บ้านเลขที่		
14	moopart	Text	3	หมู่ที่		
15	amppart	Text	30	อำเภอ		
16	tmbpart	Text	30	ตำบล		
17	road	Text	30	ถนน		
18	province_id	Text	4	รหัสจังหวัด	FK	province
19	po_code	Text	7	รหัสไปรษณีย์		
20	hometel	Text	10	เบอร์โทรศัพท์		
21	sex_id	Text	2	รหัสเพศ	FK	sex
22	Out_time	Date/Time		เวลาออกจากสถานที่		
23	marital_id	Text	3	รหัสสถานภาพ	FK	marital_status
24	fathername	Text	30	ชื่อบิดา		
25	fatherlname	Text	30	สกุลบิดา		
26	mathername	Text	30	ชื่อมารดา		
27	motherlname	Text	30	สกุลมารดา		
28	Pic_number	Text	40	รหัสรูปหน้า		

ประวัติผู้วิจัย

ชื่อ - สกุล	สมเกียรติ ดอนทองแดง
วันเดือนปีเกิด	4 เมษายน พ.ศ. 2523
ที่อยู่	49 ม.2 ต.สระสี่มุม อ.กำแพงแสน จ.นครปฐม

ประวัติการศึกษา

พ.ศ. 2534	สำเร็จการศึกษาชั้นประถมปีที่ 6 โรงเรียนวัดสระสี่มุม
พ.ศ. 2537	สำเร็จการศึกษาชั้นมัธยมศึกษาตอนต้น(ม.3) โรงเรียนมัธยมฐานบิน
พ.ศ. 2540	สำเร็จการศึกษาชั้นมัธยมศึกษาตอนปลาย(ม.6) โรงเรียนมัธยมฐานบิน
พ.ศ. 2544	สำเร็จการศึกษาปริญญาตรี สาขา คอมพิวเตอร์ธุรกิจ มหาวิทยาลัยศรีปทุม