การออกแบบและพัฒนาระบบการชำระเงิน แบบไมโครเพย์เม็นต์ทางอินเตอร์เน็ต

Design and Implement Internet Micro Payment System

โดย

นางสาวลีลาวดี เลิศสวัสดิ์

รหัส 44067094

อาจารย์ที่ปรึกษา

ผศ. ดร. โชติพัชร์ ภรณวลัย

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
ภาคเรียนที่ 2 ปีการศึกษา 2545
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	การออกแบบและพัฒนาระบบการชำระเงินแบบไมโครเพย์เม็นต์ทางอินเตอร์เน็ต
นักศึกษา	นางสาวลีลาวดี เลิศสวัสดิ์
อาจารย์ที่ปรึกษา	ผศ. ดร. โชติพัชร์ ภรณวลัย
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2545

บทคัดย่อ

การเติบโตของพาณิชย์อิเลคโทรนิกส์บน Internet ได้ทำให้มีการพัฒนาระบบและเทคนิคที่จะนำมาใช้ในการชำระเงินผ่าน Internet มากยิ่งขึ้น ทั้งนี้ไม่เพียงแค่ผลิตภัณฑ์ที่มีตามท้องตลาด (tangible products) ที่ได้ถูกนำมาค้าขายบน Internet แต่ได้เกิดผลิตภัณฑ์ประเภท intangible product เช่น รูปภาพ เพลง อิเลคโทรนิกส์การ์ด ข้อมูลเสียง ฯลฯ จึงได้มีการคิดค้นลักษณะการชำระเงินที่เหมาะสมกับผลิตภัณฑ์ประเภทนี้ขึ้น สำหรับโครงงาน Internet Micro Payment System นี้เป็นโครงงานพัฒนา Client Server Web Application ที่จำลองการทำงานของ Micro Payment โดยในระบบจำลองจะประกอบไปด้วยร้านค้า 2 ร้าน และตัวกลางที่ให้บริการ Micro Payment System ที่ทำหน้าที่เป็น server อีก 1 ตัว

Title	Design and Implement Internet Micro Payment System
Student	Miss Leelawadee Lertsawad
Advisor	Assistant Professor Dr. Chotipat Pornvalai
Level of Study	Master of Science in Information Technology
Major	Information Science
Academic Year	2002

Abstract

The evolution of e-commerce has increased the systems and technologies to enable the widespread usage of online payment technology. Not only the tangible products are sold through internet but also the intangible products as well. Example of intangible products are graphic files, electronic card, sounds etc. Suitable mechanism of online payment through internet for these kinds of product have been proposed. For this project on Internet Micro Payment System is a project that will involve the development of Client Server Web Application. The simulated system will consists of two merchants websites and a Micro Payment System Service.

กิตติกรรมประกาศ

ขอขอบคุณ ผศ. ดร. โชติพัชร์ ภรณวลัย สำหรับคำปรึกษา และขอขอบคุณครอบครัว ญาติมิตร และเพื่อนๆ ที่ให้การสนับสนุนและกำลังใจเสมอมาค่ะ

สารบัญ

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญภาพ

ภาพที่ หน้า

บทที่ 1

บทนำ

การเติบโตของพาณิชย์อิเลคโทรนิกส์บน อินเตอร์เน็ต ได้ทำให้มีการพัฒนาระบบและเทคนิคที่จะนำมาใช้ในการชำระเงินผ่าน อินเตอร์เน็ต มากยิ่งขึ้น ทั้งนี้ไม่เพียงแค่ผลิตภัณฑ์ที่มีตามท้องตลาด (tangible products) ที่ได้ถูกนำมาค้าขายบน อินเตอร์เน็ต แต่ได้เกิดผลิตภัณฑ์ประเภท intangible product ได้แก่ข้อมูลดิจิตอลประเภทต่างๆซึ่งจะกล่าวถึงต่อไป จึงได้มีการคิดค้นลักษณะการชำระเงินที่เหมาะสมกับผลิตภัณฑ์ประเภทนี้ขึ้น

ในเอกสารบทนี้จะกล่าวถึงความเป็นมาและความสำคัญของปัญหา วัตถุประสงค์ในการพัฒนาระบบงาน เป้าหมายของการพัฒนาระบบงาน ประโยชน์ที่คาดว่าจะได้รับ ขอบเขตของการพัฒนาระบบงาน ทฤษฎีที่ใช้ในการพัฒนาระบบงาน ขั้นตอนในการพัฒนาระบบงาน และสุดท้ายคือรายละเอียดของแต่ละบท

1.1 ความเป็นมาและความสำคัญของระบบ

ข้อมูลที่หลายหลากและมากมายซึ่งเปรียบเสมือนห้องสมุดขนาดใหญ่คือจุดดึงดูดและประโยชน์ของระบบอินเตอร์เน็ตข้อมูลส่วนใหญ่ไม่คิดค่าบริการเพื่อเป็นการดึงดูดให้ผู้บริโภคเข้ามาใช้บริการเว็บไซด์ของตน เหตุผลอีกประการที่ข้อมูลส่วนใหญ่ยังไม่มีการคิดค่าบริการเนื่องจากกรรมวิธีในการชำระค่าบริการในปัจจุบันไม่เหมาะสมที่จะนำมาใช้เป็นวิธีในการรับชำระค่าบริการได้ โดยเฉพาะค่าบริการที่มีมูลค่าน้อย ซึ่งนิยมเรียกว่า ไมโครเพย์เมนต์

ไมโครเพย์เมนต์ คือการชำระเงินที่มีมูลค่าต่ำเกินกว่าจะประเมินต้นทุนและค่าใช้จ่ายโดยใช้บัตร หรือ การชำระสินค้าที่มีมูลค่าต่ำกว่า 1 ดอลลาร์ หรือประมาณ 50 บาท เพราะค่าใช้จ่ายของบัตรเครดิตต่อรายการอยู่ที่ 20-25 เซนต์ หรือประมาณ 10 บาท โดยทั่วไปการชำระค่าข้อมูลสามารถทำได้ทั้งโดยแม็คโครเพย์เมนต์และโดย ไมโครเพย์เมนต์

แรกเริ่มเดิมที การชำระเงินบน อินเตอร์เน็ต นิยมใช้บัตรเครดิตกันอย่างแพร่หลาย แต่วิธีนี้จะต้องมีการหักค่าธรรมเนียม และมีการ delay ของเวลาเกิดขึ้นเพราะต้องต่อหลายระบบ ซึ่งทำให้ไม่สะดวกและไม่คุ้มค่าต่อการชำระทีละน้อยๆ ดังนั้นจึงได้เกิดทางแก้ไขที่เป็นไปได้ คือ

- ให้บริการข้อมูลโดยไม่เก็บค่าบริการ และเก็บค่าโฆษณาแทน
- ขายข้อมูลทีละมากๆ โดยอาจขายรวมกันหลายชุด เช่น เว็บประเภทนิตยสาร ก็ขายสิทธิการเข้าใช้เป็นรายปี แทนรายเล่ม หรือ เว็บให้บริการกราฟิกก็เก็บเป็นค่าสมาชิกรายปี ถึงจะได้เข้าไปใช้กราฟิก
- ชำระเป็น ไมโครเพย์เมนต์ หรือ ชำระต่อการคลิกหรือต่อการกดปุ่มนั่นเอง

การขยายตัวของ อินเตอร์เน็ต ในแง่ของความหลากหลายของประเภทข้อมูลดิจิตอลที่เกิดขึ้น เช่น ซอฟต์แวร์ ข้อมูลข่าว ข้อมูลดัชนีหุ้น เพลง รูปภาพ วีดีโอไฟล์ และ ข้อมูลค้นคว้ารายงาน ได้สร้างช่องทางใหม่ๆในการชำระเพิ่มขึ้น ซึ่งวิธีการที่จะดึงดูดผู้บริโภคจะต้องคำนึงถึงส่วนประกอบต่างๆมากมาย เช่น ราคา ขนาดไฟล์ ระยะเวลาในการดาวน์โหลด เพราะข้อมูลหล่านี้สามารถถูกนำไปลอกเลียนแบบได้ไม่ยาก และเผยแพร่ได้อย่างรวดเร็วและสะดวก

ทั้งนี้ ไมโครเพย์เมนต์ ดูจะเป็นทางออกสำหรับผลิตภัณฑ์ประเภทนี้ เพราะผู้บริโภคสามารถเลือกจ่ายได้ทีละน้อย ข้อได้เปรียบต่อผู้บริโภคเมื่อมี ไมโครเพย์เมนต์ คือผู้บริโภคไม่จำเป็นต้องซื้อเป็นแพ็คแต่สามารถซื้อแยกย่อยเฉพาะหน่วยที่ต้องการได้

1.2 วัตถุประสงค์ของโครงการ

การพัฒนาโครงงานนี้เพื่อวัตถุประสงค์ดังนี้

- เพื่อเป็นการนำทฤษฎีของ ไมโครเพย์เมนต์ ที่มีในปัจจุบัน มาพัฒนาและประยุกต์ให้เข้ากับพาณิชย์อิเลคโทรนิกส์ของเว็บไซต์ไทย
- เพื่อส่งเสริมให้เกิดการแข่งขันด้านผลิตภัณฑ์ข้อมูลออนไลน์ให้มีประสิทธิภาพยิ่งขึ้น
- เพื่อให้ผู้บริโภคมีโอกาสในการเลือกผลิตภัณฑ์มากขึ้น และอำนวยความสะดวกให้ผู้บริโภคได้มีช่องทางการชำระเงินที่หลากหลายขึ้น
- เพื่อเป็นต้นแบบให้กับการพัฒนาการชำระเงินแบบ ไมโครเพย์เมนต์ ในระบบพาณิชย์อิเลคโทรนิกส์ของเว็บไซต์ไทย

1.3 เป้าหมายของระบบงาน

- ระบบสามารถรองรับการขยายของจำนวนร้านค้าและลูกค้าในอนาคตได้
- ร้านค้าเกิดความมั่นใจในการรับชำระค่าสินค้าด้วยวิธีดังกล่าว
- ผู้บริโภคเกิดความมั่นใจในการชำระเงินด้วยวิธีดังกล่าว

1.4 ขอบเขตของระบบงาน

ระบบงานนี้มีขอบเขตการศึกษาและพัฒนาที่โฟกัสไปในจุดที่เกี่ยวกับคอนเซ็บของไมโครเพย์เมนต์ดังนี้

ส่วนประกอบของระบบ

- การไหลของเงินตั้งแต่ผู้บริโภคจนถึงมือร้านค้า
- แอพลิเคชั่น ฝั่ง server ผู้ให้บริการ ไมโครเพย์เมนต์
- กระบวนการส่งผ่านรายการข้อมูลระหว่างร้านค้าและผู้ให้บริการ
- ระบบการลงทะเบียนใช้ระบบไมโครเพย์เมนต์ของร้านค้า
- ระบบการลงทะเบียนและสั่งซื้อ e-money (coupon) ของผู้บริโภค
- ระบบการสร้าง ไมโครเพย์เมนต์ e-money (coupon)
- ระบบการแลกเปลี่ยน e-money (coupon) ในระหว่างการสั่งซื้อและชำระออนไลน์
- การรับสินค้าหลังการชำระราคา
- ระบบการรายงานผลการดำเนินงานของร้านค้า
- ระบบการตรวจสอบการทำรายการของลูกค้า

ทั้งนี้การออกแบบได้รองรับการทำธุรกรรมต่างๆกับทางธนาคารเพื่อความเหมาะสมในการทำให้โฟลสมบูรณ์ แต่ส่วนการเชื่อมต่อกับทางธนาคารในส่วนต่างๆ จะไม่อยู่ในขอบเขตของการศึกษาระบบงานนี้

1.5 ทฤษฎีที่ใช้ในการพัฒนาระบบงาน

- หลักการของการชำระเงินผ่านอินเตอร์เน็ตในพาณิชย์อิเลคโทรนิกส์
- หลักการและคุณสมบัติของ ไมโครเพย์เมนต์ โปรโตคอล
- การทำงานของระบบ client server

- การทำงานของ web server และ server side script แอพลิเคชั่น
- การทำงานของ Secure Socket Layer
- การทำงานของระบบฐานข้อมูลเชื่อมกับ server side script

1.6 ขั้นตอนการดำเนินการโครงการ

ศึกษากรรมวิธีการทำงานของระบบ ไมโครเพย์เมนต์ ในทฤษฎีต่างๆ ที่มีในปัจจุบัน ได้แก่

- วิเคราะห์และออกแบบระบบงาน
- ศึกษาและคัดเลือกเทคโนโลยีที่เหมาะสมในการพัฒนาระบบ
- พัฒนาโปรแกรม
- ทดสอบระบบงาน และปรับปรุงแก้ไข
- ติดตั้งระบบเพื่อนำไปใช้งาน

1.7 รายละเอียดของแต่ละบท

ในแต่ละบทที่ประกอบกันเป็นเนื้อหาของเอกสารประกอบโครงการ สามารถสรุปรายละเอียดได้ดังนี้

บทที่ 1 เป็นบทที่กล่าวถึงที่มาของแรงจูงใจในการเลือก วัตถุประสงค์ ขั้นตอนการศึกษา ตลอดจนผลที่คาดว่าจะได้รับของการพัฒนาระบบ

บทที่ 2 กล่าวถึงรายละเอียดโดยสังเขปของหลักการและทฤษฎีที่เกี่ยวข้องในการพัฒนาระบบ

บทที่ 3 กล่าวถึงการออกแบบระบบ รวมถึงโครงสร้าง (Architecture) ของระบบ โดยวิเคราะห์ความต้องการของระบบเพื่อนำไปสู่กระบวนการพัฒนาระบบต่อไป

บทที่ 4 แสดงรายละเอียดในการพัฒนาระบบตามที่ได้ออกแบบมาในสภาพแวดล้อมที่กำหนดไว้

บทที่ 5 สรุปผลที่ได้จากการทำงานของโปรแกรม รวมถึงข้อเสนอแนะ

บทที่ 2
หลักการและทฤษฎีของระบบ

2.1 หลักการของไมโครเพย์เมนต์

2.1.1 คุณสมบัติของสินค้าที่ใช้ซื้อขายได้โดยไมโครเพย์เมนต์

- **สินค้าประเภทจับต้องไม่ได้**

ลักษณะของสินค้าที่จับต้องไม่ได้บนอินเตอร์เน็ตมีตัวอย่างให้พบเห็นได้มากมาย เช่น ข้อมูลภาพ ได้แก่ไอคอน รูปภาพ (photo stock) รูปภาพแกลอรี่ เป็นต้น ข้อมูลเสียง ได้แก่ เสียงประกอบสั้นๆ เสียงเพลง เสียงพูด เสียงข่าว เป็นต้น ข้อมูลเพื่อการค้นคว้า บทความทางวิชาการ หนังสืออิเลคโทรนิกส์ (e-book) สินค้าประเภทนี้ล้วนต้องการความเร็วในการประมวลผลการชำระเงินเพื่อทราบผลการทำรายการในทันที เพื่อให้สามารถได้รับสินค้าแบบออนไลน์ได้ในเวลาอันรวดเร็ว

- **สินค้าที่มีราคาค่างวดน้อย คืออยู่ระหว่างฟรีและแพง**

เนื่องจากสินค้ามีราคาต่ำดังนั้นกระบวนการทำรายการชำระเงินค่าสินค้าควรจะมีต้นทุนต่ำด้วย และควรมีประสิทธิภาพที่คุ้มค่าเหมาะสมกับกำไรที่จะได้ค่าสินค้านั้นๆ การที่จะชำระเงินแบบออนไลน์โดยบัตรเครดิตหรือโอนเงินผ่านบัญชีธนาคารจึงเป็นเรื่องที่ไม่เหมาะสมกับสินค้าลักษณะดังกล่าวเนื่องจากต้นทุนต่อรายการอาจจะมีมูลค่าสูงกว่าราคาสินค้า

2.1.2 บทบาทของแต่ละหน่วยในระบบ

- **โบรกเกอร์**

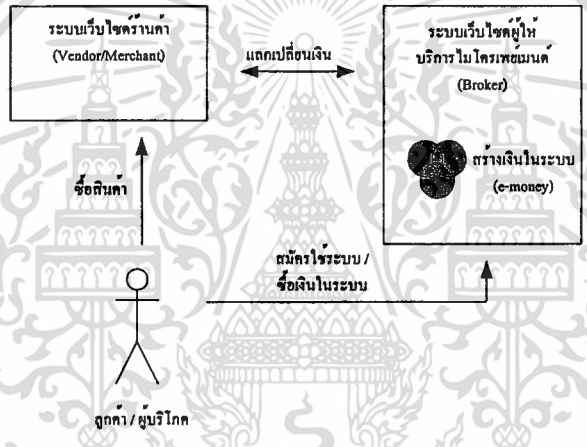
ตัวแทนของร้านค้า (เวนเดอร์) ในการจำหน่ายเงินอิเลคโทรนิกส์ที่จะใช้ในระบบ เช่น e-money สคริป หรือเหรียญ เป็นต้น โบรกเกอร์จัดเป็นสื่อกลางระหว่างร้านค้าและลูกค้า ทำหน้าที่สร้างหรือแปลงและอนุมัติเงินอิเลคโทรนิกส์ให้กับลูกค้าเพื่อให้ซื้อจากร้านค้าแต่ละเจ้าได้ โบรกเกอร์ 1 เจ้าสามารถให้บริการกับร้านค้าและลูกค้าได้มากกว่า 1 ที่

- **ลูกค้า (ผู้บริโภค)**

ผู้ซื้อสินค้าบนอินเตอร์เน็ต จะต้องติดต่อกับโบรกเกอร์เพื่อซื้อหรือแลกเงินอิเลคโทรนิกส์สำหรับใช้จ่ายในระบบ

- **ร้านค้า (เวนเดอร์)**

ผู้ขายสินค้าบนอินเตอร์เน็ต หรือเจ้าของเว็บไซต์ จะต้องให้รูปแบบในการสร้างเงินอิเลคโทรนิกส์ให้กับโบรกเกอร์เพื่อให้โบรกเกอร์สร้างเงินอิเลคโทรนิกส์ที่จะสามารถนำมาใช้จ่ายในเวบไซต์ของตนได้



รูปที่ 2.1 แสดงโครงสร้างของแต่ละหน่วยงานในระบบ

2.1.3 แนะนำองค์ประกอบการทำงานของไมโครเพย์เม็นต์

องค์ประกอบที่พบเห็นโดยทั่วไปในการทำงานของไมโครเพย์เม็นต์โปรโตคอลมีดังนี้

- **การสร้างเงินอิเลคโทรนิกส์ (Money Generation)**

มีได้สองวิธีคือ

วิธีที่ 1: เงินอิเลคโทรนิกส์ถูกสร้างหรือรับรองโดยโบรกเกอร์

ลูกค้าจะต้องทำการซื้อเงินอิเลคโทรนิกส์ที่จะใช้ในระบบไมโครเพย์เม็นต์เป็นจำนวนมากผ่านการชำระเงินแบบแมคโครเพย์เม็นต์กับโบรกเกอร์ก่อน วิธีการนี้ถูกจัดเป็นแบบเดบิตเบส

(debit-based) เนื่องจากลูกค้าจะต้องจ่ายเงินล่วงหน้าให้กับตัวแทนจำหน่ายเงินอิเลคโทรนิกส์ในไมโครเพย์เม็นต์ โดยผู้ที่เป็นฝ่ายได้เงินจะเป็นผู้ที่ได้รับผลประโยชน์จากการเหลือของเศษเงินอิเลคโทรนิกส์ที่ใช้ไม่หมด ทั้งนี้นโยบายการคืนเงินอิเลคโทรนิกส์ หรือการนำเงินอิเลคโทรนิกส์เก่าไปแลกเป็นเงินอิเลคโทรนิกส์ใหม่จึงต้องมีขึ้น

วิธีที่ 2: เงินอิเลคโทรนิกส์ถูกสร้างโดยผู้ซื้อ

วิธีการนี้จะไม่มีการชำระเงินก้อนใหญ่ล่วงหน้าโดยลูกค้า จัดว่าเป็นเครดิตเบส (credit-based) แบบหนึ่งที่เงินจากบัญชีลูกค้าจะไม่ถูกตัดออกไปจนกว่าจะมีการแลกเปลี่ยนสินค้าเกิดขึ้น โดยเงินอิเลคโทรนิกส์ที่เกิดขึ้นจากลูกค้าจะต้องได้รับการอนุมัติสิทธิ์ในการสร้างก่อน

- **การตรวจจับรายการซ้ำจากเงินที่ได้ถูกใช้แล้ว (Double Spending Detection)**

เนื่องจากเงินในไมโครเพย์เม็นต์เป็นการรวมกันของบิตของข้อมูล ดังนั้นการนำเงินดังกล่าวไปใช้ในระบบไมโครเพย์เม็นต์แบบต่างๆ จึงมีความจำเป็นที่จะต้องมีส่วนของการตรวจจับข้อมูลเงินดังกล่าวในฐานข้อมูลของระบบก่อนถึงขั้นตอนการชำระ เพื่อป้องกันการถูกนำมาใช้ซ้ำ ซึ่งจะทำให้ผู้ขายเสียผลประโยชน์

- **การแลกเงินอิเลคโทรนิกส์คืน (Redemption)**

ส่วนของการแลกเงินอิเลคโทรนิกส์คืนในไมโครเพย์เม็นต์จัดเป็นการทำงานออฟไลน์ที่ลูกค้าต้องประสานงานกับโบรกเกอร์เอง

- **การจ่ายก่อนหรือหลัง (Pay-before or pay-after)**

ขั้นตอนของการชำระเงินอิเลคโทรนิกส์ (ค่าสินค้า) ก่อนหรือหลังการได้รับสินค้าจัดว่าเป็นปัจจัยที่ไม่มีผลต่อการทำงานของไมโครเพย์เม็นต์

- **ขีดจำกัดของเวลา (Notion of time)**

เนื่องจากว่าการใช้จ่ายด้วยเงินอิเลคโทรนิกส์เป็นสิ่งจำเป็นในไมโครเพย์เม็นต์ ดังนั้นจึงต้องมีการกำหนดอายุการใช้งานของเงินอิเลคโทรนิกส์ เพื่อป้องกันภาวะการแข่งขันไม่ให้เกิดขึ้น

2.1.4 ความเสี่ยงของระบบ

ในการทำธุรกรรมบนอินเตอร์เน็ตในลักษณะเป็นไมโครเพย์เมนต์สามารถเผชิญกับความเสี่ยงดังต่อไปนี้

- **การใช้เครดิตในทางมิชอบ (Credit Abuse)**

  กล่าวคือ ผู้ที่สามารถเข้าถึง account ของ user ทำรายการโดยใช้เครดิตของ user ในทางมิชอบ user ไม่มีความตั้งใจจะชำระเงินแต่แอบโดนกระทำธุรกรรม

- **การปลอมแปลง (Counterfeiting)**

  มีธุรกรรมปลอมเกิดขึ้น

- **การถอนหรือเบิกจากบัญชีโดยไม่ได้รับอนุญาติ (Unauthorized Withdrawal)**

  มีการทำการเบิกมูลค่ารายการจากบุคคลผู้ไม่มีสิทธิ

- **การเปลี่ยนแปลงข้อมูลการสั่งซื้อ (Purchase Order Modification)**

  เมื่อลูกค้าต้องการสั่งซื้อสินค้า แต่ถูกบุคคลภายนอกแทรกแซง โดยแอบเปลี่ยนแปลงรายการข้อมูลการสั่งซื้อไปจากความเป็นจริง

- **ล้มเหลวในการชำระรายการ (Failure to Credit Payment)**

  ผู้ให้บริการหักเงินจากลูกค้า แต่ไม่ให้ยอดเงินกับผู้ขาย

- **การชำระซ้ำ (Double Spending)**

  การสั่งจ่ายถูกกระทำซ้ำ ไม่ว่าจะจากตัวลูกค้าเอง ร้านค้า หรือ บุคคลที่สาม

- **ถูกปฏิเสธการใช้งาน (Denial of Service)**

  ลูกค้าหรือร้านค้าถูกระงับสิทธิการใช้ระบบ

- **การปฏิเสธ (Repudiation)**

  ฝ่ายใดฝ่ายหนึ่งปฏิเสธการทำรายการ

- **ส่งสินค้าไม่สำเร็จ (Failure to Deliver)**

  ร้านค้ารับรายการชำระ แต่มีปัญหาด้านการส่งสินค้า

- **การใส่ความ (Framing)**

  ความสามารถในการทำให้ชวนเชื่อได้ว่าบุคคลที่สามกระทำความผิด

2.1.5 ความต้องการของระบบ ไมโครเพย์เมนต์ (Micropayment Requirements)

ก. ความต้องการทางด้านธุรกิจ

1. มุมมองผู้บริโภค

การเชิญชวนให้ผู้บริโภคหันมาใช้การชำระเงินแบบใหม่นั้นเป็นเรื่องที่สำคัญและท้าทายต่อระบบไมโครเพย์เมนต์ เป็นอย่างมาก

จุดสำคัญที่ต้องพิจารณาคือ

- ความสะดวกของการติดตั้ง

กล่าวคือการติดตั้งควรมีขั้นตอนที่ผู้บริโภคต้องปฏิบัติให้น้อยที่สุด

- ง่ายต่อการใช้งาน

ตลอดจนขั้นตอนการลงทะเบียนขอใช้ระบบของผู้บริโภคจะต้องกระชับและตรงไปตรงมา

- ความเหมาะสมด้านราคาสินค้า

เนื่องจากความเคยชินของผู้บริโภคกับการมีเว็บบราวเซอร์ ตลอดจนแอพลิเคชั่นพลักอินที่ลงได้ฟรีและง่าย จึงเป็นไปได้ยากที่จะขายสินค้าประเภทข้อมูลดิจิตอลผ่านอินเตอร์เน็ตโดยมีกำไรมาก

ความปลอดภัยของผู้บริโภคจากการถูกโกง

ข้อมูลส่วนตัวต่างๆของผู้บริโภคจะต้องเก็บเป็นความลับ จะเห็นว่าการใช้บัตรเครดิตในการชำระค่าสินค้าเป็นจุดที่ด้านทานความดึงดูดในการซื้อสินค้าผ่าน อินเตอร์เน็ต อย่างมาก เพราะการเปิดเผยข้อมูลบัตรเครดิตออกไปบนอินเตอร์เน็ตเป็นการเสี่ยงต่อการถูกนำข้อมูลไปประกอบการฉ้อโกงหรือทุจริตได้ แม้ว่าจะมีการคิดค้นความปลอดภัยระบบต่างๆขึ้นมา เช่น SSL ก็ตาม

- ความเป็นส่วนตัวของข้อมูลของผู้บริโภค

การลงทะเบียนในเว็บต่างๆ ไม่ว่าจะเพื่อการเข้าไปเป็นสมาชิก ใช้งานเว็บ ใช้ระบบชำระเงิน ข้อมูลเบอร์บัตรเครดิตที่ใช้ในการชำระนั้นๆ ซึ่งถูกเก็บไว้ในระบบฐานข้อมูลเอง หรือแม้กระทั่งพฤติกรรมการจับจ่ายใช้สอยของผู้บริโภคที่อาจถูกเก็บบันทึกเพื่อวิเคราะห์แนวโน้มทางการตลาด ล้วนเกี่ยวข้องกับการเปิดเผยข้อมูลส่วนตัวบางส่วนของผู้บริโภคออกไป โดยองค์กรต่างๆที่เก็บข้อมูลเหล่านี้จะต้องมีการควบคุมความปลอดภัยของข้อมูลอย่างเคร่งครัด ความสามารถในการป้องกันข้อมูลดังกล่าวก็เป็นจุดที่สำคัญในมุมมองของผู้บริโภคเช่นกัน

อย่างไรก็ตามความสำเร็จของระบบ ไมโครเพย์เมนต์ เองก็ขึ้นอยู่กับความน่าสนใจของตัวสินค้า จะต้องมีความดึงดูดที่ครอบคลุมความต้องการต่างๆที่ได้กล่าวมาข้างต้น จึงจะทำให้ระบบประผลสำเร็จได้

- ความสะดวกของผู้บริโภค

ผู้บริโภคไม่จำเป็นต้องสมัครเป็นสมาชิกเว็บไซด์ต่างๆ ที่ให้บริการข่าวสารบทความ ซึ่งจะต้องใช้เงินมากในการสมัครให้ครบทุกเว็บที่มีบทความที่อยู่ในความสนใจของผู้บริโภค และต้องมาคอยจดจำรหัสผ่านเพื่อใช้ login เว็บไซด์ต่างๆเหล่านั้น แต่ผู้บริโภคสามารถเลือกดาวน์โหลดเมื่อพบเฉพาะบทความที่ตัวเองสนใจซึ่งจะเสียค่าใช้จ่ายน้อยกว่ามาก โดยไม่ต้องสมัครเป็นสมาชิกเว็บไซด์เหล่านั้นซึ่งส่วนใหญ่จะต้องให้ข้อมูลเบอร์บัตรเครดิตไว้ก่อน

2. มุมมองพ่อค้า

จุดสำคัญในมุมมองของพ่อค้าคือ

- รายได้ที่เพิ่มขึ้น

การขยายช่องทางการตลาดของสินค้าออกไปบนอินเตอร์เน็ตเป็นการเพิ่มรายได้อีกทางของพ่อค้า เนื่องจากตลาดที่ใหญ่ขึ้น ทั่วโลก และยังขายได้ตลอด 24 ชั่วโมง

แม้ว่าปัจจุบันผู้บริโภคสามารถซื้อข้อมูลดิจิตอลผ่านอินเตอร์เน็ตได้สะดวกขึ้นก็ตาม ผู้บริโภคยังคงต้องปฏิบัติตามแนวการจัดจำหน่ายของร้านค้า เช่น ซื้อเสียค่าสมัครสมาชิกรายปี หรือ ซื้อในปริมาณมาก ซึ่งแนวทางดังกล่าวจะจำกัดตลาดให้อยู่เฉพาะในวงของผู้บริโภคที่มีลักษณะเป็นสถาบัน องค์กร หรือ ผู้ยินยอมใช้เงินทีละมากๆได้เท่านั้น ยกตัวอย่างเช่น วอลล์สตรีทเจอนัล (Wall Street Journal) ซึ่งให้บริการข้อมูลข่าว รายงานการค้นคว้า ข่าวสารการตลาด และข่าวสารการลงทุน โดยคิดค่าสมัครสมาชิกรายปีถึงปีละ $59 ต่อปี อย่างไรก็ตามทางวอลล์สตรีทเจอนัลได้ร่วมกับบริษัทคิวพาสเพื่อนำเทคโนโลยีไมโครเพย์เมนต์มาใช้ โดยให้ผู้บริโภคสามารถเลือกซื้อสินค้าเฉพาะที่ต้องการได้โดยไม่ต้องสมัครสมาชิกรายปี แนวโน้มที่เปลี่ยนแปลงดังกล่าวจะทำให้พาณิชย์อิเลคโทรนิกส์สามารถก้าวไปสู่ตลาดที่กว้างขึ้นในสายของสินค้าที่ร้านค้าแต่ละเจ้ามีได้ ระบบไมโครเพย์เมนต์ยังสามารถทำให้ผู้ค้าขายปลีกออนไลน์ นำสินค้าที่มีความหลากหลายมาสู่ท้องตลาด เช่น ข่าว ซอฟ์ตแวร์ รายงานค้นคว้า บทความทางวิชาการ บทความตีพิมพ์ทางราชการ ไฟล์เพลง MP3 หนังสือดิจิตอล เอกสารดิจิตอล รูปภาพ ไฟล์วีดีโอ เช่าหนัง เป็นต้น และแน่นอน

บริการออนไลน์ทั้งหมดรวมไปถึงโทรศัพท์และโทรสาร วีดีโอคอนเฟอเร็นซ์ การบริหารการเงิน การเพิ่มตลาดใหม่ๆเหล่านี้ย่อมนำมาสู่ทางเลือกที่ดีขึ้นของลูกค้า

- ลดค่าใช้จ่าย

การลดค่าใช้จ่ายก็เป็นส่วนสำคัญสำหรับผู้ค้าปลีก พาณิชย์อิเลคโทรนิกส์ รายย่อยที่จะทำการตัดสินใจเลือกใช้ ระบบไมโครเพย์เมนต์นอกเหนือไปจากโอกาสในการเพิ่มรายได้ ค่าใช้จ่ายสำหรับผู้ค้าปลีกสามารถแบ่งได้เป็น 3 ประเภทได้แก่ ค่าใช้จ่ายในการติดตั้ง ค่าใช้จ่ายในการบำรุงรักษาและรองรับจำนวนผู้ใช้ที่เพิ่มขึ้น และค่าใช้จ่ายที่เกิดเนื่องจากความปลอดภัย (security) ที่มีไม่เพียงพอ สำหรับค่าใช้จ่ายในการติดตั้งนั้น แม้ว่าจะไม่ค่อยเป็นประเด็นที่สำคัญสำหรับผู้ประกอบการ พาณิชย์อิเลคโทรนิกส์ รายใหญ่ แต่จะมีความสำคัญอย่างมากสำหรับผู้ประกอบการรายย่อย ดังนั้นแล้วถ้าสามารถที่จะ outsource บริการไมโครเพย์เมนต์แก่ผู้ประกอบการรายย่อยได้ก็จะทำให้เป็นข้อได้เปรียบสำหรับไมโครเพย์เมนต์ เนื่องจากผู้ประกอบการรายย่อยจะได้ไม่ต้องรับค่าใช้จ่ายในการติดตั้งในตอนเริ่มให้บริการจากการติดตั้งระบบรวมถึงบุคคลากรผู้ชำนาญในด้านนี้ด้วย

สำหรับค่าใช้จ่ายในการบำรุงรักษาและรองรับจำนวนผู้ใช้ที่เพิ่มขึ้นนั้นจะมีส่วนสำคัญสำหรับผู้ค้าปลีก พาณิชย์อิเลคโทรนิกส์ ทุกราย ในด้านของการบำรุงรักษา ผู้ให้บริการ พาณิชย์อิเลคโทรนิกส์ทุกรายต้องการให้ระบบ มีความเชื่อถือได้เป็นอย่างสูงไม่จำเป็นต้องมีบุคคลากรคอยควบคุมอยู่ตลอดเวลา ในส่วนของการรองรับ จำนวนผู้ใช้ที่เพิ่มขึ้นนั้นเป็นความสามารถที่เป็นที่สนใจสำหรับทั้งผู้ประกอบการรายใหญ่และรายย่อย

สุดท้ายนี้ในส่วนของค่าใช้จ่ายเนื่องจากระบบมีความปลอดภัย (security) ไม่พอเพียงนั้น จากการศึกษาระบบ พาณิชย์อิเลคโทรนิกส์ ในปัจจุบันพบว่าร้อยละสิบของการใช้จ่ายในระบบ พาณิชย์อิเลคโทรนิกส์ นั้น มีการปลอมแปลงหรือลักลอบใช้รหัสบัตรเครดิต ซึ่งการปลอมแปลงและการลักลอบใช้นี้ จะทำให้ผู้ให้บริการต้องแบกรับภาระค่าใช้จ่ายในส่วนนั้น รวมทั้งยังมีผลต่อการเติบโตของระบบ พาณิชย์อิเลคโทรนิกส์

- ความปลอดภัย (security) และประสิทธิภาพของระบบ (performance)

ในปัจจุบันเทคโนโลยีที่ทำให้การรับส่งข้อมูลมีความปลอดภัยที่ใช้กันอยู่คือการเข้ารหัส (encryption) แต่เทคโนโลยีนี้มีความจำเป็นจะต้องทำการคำนวณ ซึ่งทำให้มีผลต่อการส่งข้อมูลแบบ real-time อย่างสูง นอกจากนี้วิธีการในการตรวจสอบผู้ใช้และผู้ให้บริการ ก็จำเป็นจะต้องมีขั้นตอนในการพิสูจน์หลายขั้นตอน ซึ่งมีผลต่อความซับซ้อนของ software และประสิทธิภาพของ

server โดยทั่วไปแล้ว trade-off ระหว่างความปลอดภัย (security) ประสิทธิภาพ (performance) และ ความซับซ้อน (complexity) จะเป็นส่วนสำคัญในการพิจารณาระบบไมโครเพย์เมนต์ต่างๆ

- มาตรฐานที่เปิด (Open Standard) และ การใช้ผลิตภัณฑ์จากหลายผู้ผลิต

เนื่องจากการที่จะต้องพึ่งพาผู้ผลิตรายเดียวในระบบที่สำคัญอย่าง พาณิชย์อิเลคโทรนิกส์ นั้น จะเป็นการเสี่ยงสำหรับผู้ให้บริการ ดังนั้นการใช้มาตรฐานที่เปิดสำหรับระบบไมโครเพย์เมนต์ รวมถึงอุปกรณ์มาตรฐานต่างๆ จึงมีความจำเป็น เนื่องจากสามารถทำให้ใช้ผลิตภัณฑ์จากผู้ผลิตต่างๆกันได้ MasterCard และ Visa ได้มีความพยายามในการเสนอมาตรฐาน Secure Electronic Transaction (SET) โดยการกำหนดมาตรฐานในการเชื่อมต่อ (interface standard) ทั้งยังมีการออกรายชื่อผู้ผลิตสำหรับอุปกรณ์ต่างๆ ตามระบบ SET อย่างเป็นทางการ

แต่ในทางตรงกันข้าม ผู้ผลิตก็พยายามที่จะให้ผู้ให้บริการใช้อุปกรณ์จากทางผู้ผลิตเองแต่เพียงรายเดียว เพื่อความได้เปรียบ โดยทั่วไปแล้ว ความสมดุลย์ในการผสมผสานระหว่าง ความพยายามในการสร้างมาตรฐานของตัวเอง เพื่อให้ผู้ที่ซื้อระบบซื้อจากทางผู้ผลิตแต่เพียงรายเดียว กับการมีส่วนร่วมในระบบมาตรฐานที่เปิดจะเป็นส่วนสำคัญยิ่งสำหรับผู้ผลิตอุปกรณ์ระบบไมโครเพย์เมนต์ในเชิงกลยุทธทางการค้า

ข. ความต้องการทางด้านเทคโนโลยี

เทคโนโลยีที่ช่วยให้ ไมโครเพย์เมนต์ เป็นจริงขึ้นมาได้ นับตั้งแต่ Smart Card ไปจนถึง Software หรือ ทั้งสองอย่างรวมกันยังอยู่เพียงในขั้นเริ่มต้นเท่านั้น ซึ่งมีผลทำให้การพัฒนาของ ไมโครเพย์เมนต์ technology เป็นไปอย่างล่าช้า ขั้นตอนในการพัฒนามาตรฐานและรับเอาความคิดริเริ่มต่างๆ ในปัจจุบัน จะเป็นสิ่งสำคัญที่ทำให้ ไมโครเพย์เมนต์ เป็นที่แพร่หลายในหมู่ผู้ใช้ในอนาคต นอกจากนี้เทคโนโลยีอื่นๆ ที่สำคัญจะต้องถูกพิจารณาอย่างถี่ถ้วน รวมทั้ง ความปลอดภัย (security), ความสามารถในการรองรับจำนวนผู้ใช้ที่เพิ่มขึ้น (scalability) และ การแลกเปลี่ยนข้อมูลแบบ real-time (real-time transaction) เทคโนโลยีเสริมอื่นๆ ที่อาจเป็นส่วนประกอบ หรือส่วนเติมเต็ม เช่น การสื่อสารความเร็วสูง (broadband connectivity) และ การเข้ารหัส (encryption) ก็จะมีส่วนเกี่ยวข้องด้วยเช่นกัน เนื้อหาในบทนี้จะกล่าวถึงเทคโนโลยีที่สำคัญและที่เป็นส่วนเติมเต็มดังกล่าว รวมถึง ความสามารถของ ไมโครเพย์เมนต์ technology ในอนาคต

เทคโนโลยีที่สำคัญ

- ความปลอดภัย (security)

ความปลอดภัยของเทคโนโลยีเป็นสิ่งที่สำคัญ และจะมีผลต่อความนิยมแพร่หลายของ ไมโครเพย์เมนต์ technology เพราะโดยปกติผู้ใช้จะมีความกังวลว่าข้อมูลส่วนตัวหรือรหัสประจำตัวจะถูกขโมยและลักลอบนำไปใช้ ในส่วนของบริษัทผู้ให้บริการก็ไม่สามารถที่จะรู้ได้ว่าผู้สั่งสินค้าหรือบริการจะเป็นเจ้าของรหัสนั้นๆจริงหรือไม่

Digital Certificate (DC) ซึ่งเปรียบเหมือนบัตรประจำตัวแบบ electronic เป็นเทคโนโลยีที่ถูกใช้ในการตรวจสอบและพิสูจน์ผู้ใช้ DC จะถูกสร้างขึ้นใน software และใช้เป็นตัวพิสูจน์ผู้ใช้หรือเครื่องคอมพิวเตอร์ โดยจะสามารถบรรจุไว้ใน smart card หรือ hard drive ของเครื่องคอมพิวเตอร์ก็ได้ Certificate Authority จะเป็นผู้ให้ DC กับผู้ใช้ และจะเป็นผู้ที่รับรองความปลอดภัยให้กับทั้งสองฝ่าย โดย Certificate Authority อาจจะเป็นธนาคาร, หน่วยงานของรัฐ หรือว่า จะเป็น ผู้ให้บริการเครดิตการ์ดก็ได้ Certificate Authority จะตรวจสอบ DC และจะคอยตรวจสอบรหัสผ่านของผู้ใช้ ข้อดีของการใช้ Digital Certificate คือ มีความปลอดภัยมากกว่าการใช้รหัสผ่านเพียงอย่างเดียว และผู้ใช้ก็จะสามารถลดค่าใช้จ่ายในการบำรุงรักษาในส่วนของ security layer ลงได้ ข้อเสียสำคัญอีกอย่างหนึ่งของ Digital Certificate คือ โปรแกรมที่ต่างกัน เช่น Navigator กับ Explorer ก็จะต้องการ Certificate ที่แตกต่างกัน ทำให้ผู้ใช้อาจถูกปฏิเสธจาก Certificate Authority ได้เมื่อเปลี่ยนโปรแกรมที่ใช้ ซึ่งในปัจจุบันก็ได้มีการแข่งขันกันเพื่อที่จะพยายามทำ Certificate ให้เป็นมาตรฐานเพื่อแก้ไขข้อเสียนี้ โดย Microsoft ได้ทำการเสนอ อินเตอร์เน็ต Security Framework ขึ้น ส่วนทาง Intel ก็ได้เสนอ Common Data Security Architechture ขึ้น ข้อเสียอีกอย่างสำหรับ Digital Certificate คือ DC อาจจะถูกนำไปใช้โดยผู้อื่นที่ไม่ได้รับอนุญาต ได้ เนื่องจาก DC ถูกเก็บอยู่ในรูปของ software ทางแก้ไขทางหนึ่งก็คือการใช้ smart card ซึ่งจะสามารถเพิ่มความปลอดภัยให้ผู้ใช้ได้ เนื่องจาก Certificate จะถูกเก็บอยู่ในการ์ด ซึ่งผู้ใช้สามารถนำไปใช้ในเครื่องใดก็ได้

ในส่วนของการป้องกันในการรับส่งข้อมูล ก็จะมีการใช้ Secure Socket Layer (SSL) โปรโตคอลบน อินเตอร์เน็ต ซึ่งโปรโตคอล SSL นี้ จะทำการเข้ารหัสข้อมูล http บน TCP/IP ทำให้ผู้ใช้สามารถวางใจในการส่งข้อมูลที่เป็นความลับได้ SSL โปรโตคอลนี้เองก็มีอยู่ในโปรแกรม browser โดยส่วนใหญ่

- ความสามารถในการรองรับจำนวนผู้ใช้ที่เพิ่มขึ้น (Scalability)

ความสามารถในการรองรับจำนวนผู้ใช้ที่เพิ่มขึ้นนี้หมายถึงความสามารถปรับตัวให้รับกับจำนวนข้อมูลที่เพิ่มมากขึ้น รวมถึงการเปลี่ยนแปลงรูปแบบในเชิงธุรกิจ บริการที่รองรับความสามารถนี้จะสามารถตรวจดูเงื่อนไขทางธุรกิจหรือจำนวนข้อมูล และบริษัทผู้ให้บริการก็จะสามารถปรับเปลี่ยนรูปแบบเพื่อรองรับความต้องการของผู้ใช้บริการได้

ความสามารถในการรองรับจำนวนผู้ใช้ที่เพิ่มขึ้นของ server ที่ให้บริการ แอพลิเคชั่น นั้นจะเป็นส่วนประกอบที่สำคัญในด้านการตลาด เนื่องจาก พาณิชย์อิเลคโทรนิกส์ น่าจะมีการเจริญเติบโตอย่างยิ่งในระยะเวลาสองสามปีนับจากนี้ รวมทั้งเนื่องจากการไหลของข้อมูลเป็นไปอย่างไม่มีรูปแบบ ดังนั้น server จึงจำเป็นต้องสามารถรองรับปริมาณข้อมูลได้เป็นจำนวนมาก ในปัจจุบันเนื่องจาก NT Server ไม่สามารถรองรับจำนวนผู้ใช้จำนวนมากๆ ได้ รวมทั้งมี bug เป็นจำนวนมาก ทำให้ Unix เป็นที่นิยมมากกว่าในด้าน พาณิชย์อิเลคโทรนิกส์ และ การใช้งานด้าน financial ต่างๆ ถึงแม้ว่าจะมีค่าบำรุงรักษาที่สูงกว่า ดังนั้นจึงเห็นได้ว่า scalability เป็นสิ่งจำเป็นที่จะต้องคำนึงถึงก่อนที่ก่อนที่การใช้งานด้าน พาณิชย์อิเลคโทรนิกส์ (รวมถึง พาณิชย์อิเลคโทรนิกส์ สำหรับ ไมโครเพย์เมนต์) จะเป็นที่แพร่หลาย

- การแลกเปลี่ยนข้อมูลแบบ real-time (real-time tranaction)

ความสามารถนี้เป็นอีกส่วนประกอบหนึ่งที่สำคัญของระบบ พาณิชย์อิเลคโทรนิกส์ ว่าจะทำให้ผู้ให้สินค้าหรือบริการยอมรับ ไมโครเพย์เมนต์ หรือไม่ โดยทั่วไปแล้วผู้ให้สินค้าหรือบริการต้องการที่จะได้รับค่าตอบแทนจากผู้ที่ใช้บริการโดยทันทีเพื่อลดความเสี่ยงที่จะไม่ได้รับค่าตอบแทนลง ขณะนี้ Online Resource & Communications Corporation ได้ร่วมมือกับ CyberCash ในการทำระบบแบบ real-time ที่จะทำให้ผู้ใช้ซื้อสินค้าสามารถได้รับอนุมัติในการใช้เงินได้ในทันทีโดยการตรวจสอบจากบัญชีธนาคารโดยตรงก่อนที่ผู้ใช้จะสามารถใช้ CyberCash ได้ และเมื่อผู้ใช้ได้ตกลงจะจ่ายเงินแล้วเดบิตในบัญชีของผู้ใช้จะถูกหักลงในทันที แล้วทาง CyberCash ก็จะทำการส่งค่าตอบแทนนั้นไปให้ทางผู้ให้สินค้าหรือบริการ

เทคโนโลยีเสริม

ในทางด้าน พาณิชย์อิเลคโทรนิกส์ ไมโครเพย์เมนต์ ผู้ให้บริการเสริมในด้านต่างๆ จะมีส่วนเข้ามาเกี่ยวข้อง โดยเฉพาะผู้ให้บริการการเข้ารหัส (encryption) และผู้ให้บริการการสื่อสารความเร็วสูง (broadband connectivity)

- การเข้ารหัส (encryption)

ดังที่ได้กล่าวไว้แล้วข้างต้น ความปลอดภัยเป็นสิ่งจำเป็นสำหรับ ไมโครเพย์เมนต์ technology ดังนั้นจึงมีโอกาสเป็นไปได้สูงมากที่ผู้ให้บริการการเข้ารหัส (encryption) จะมีส่วนเกี่ยวข้องในการให้บริการเสริมกับเทคโนโลยีนี้ หนึ่งในผู้ให้บริการด้านนี้ได้แก่ บริษัท RSA Data Security ซึ่งเป็นผู้นำทางด้านระบบการเข้ารหัสนี้ และได้ถูกนำไปใช้ใน Microsoft Windows, Netscape Navigator, Intuit's Quicken รวมทั้งผลิตภัณฑ์อื่นๆ อีกมากมาย โดยเทคโนโลยีของบริษัท RSA นี้จะฝังตัวอยู่ใน Secure Socket Layer (SSL) ซึ่งถูกพัฒนาโดย Netscape ดังนั้นจึงมีแนวโน้มที่เทคโนโลยีนี้จะเป็นส่วนประกอบในระบบ ไมโครเพย์เมนต์ อีกบริษัทที่มีแนวโน้มที่จะมีส่วนเกี่ยวข้องในเทคโนโลยีเสริมนี้ได้แก่ บริษัท Intertrust ซึ่งได้ทำการพัฒนา Metatrust software ซึ่งอนุญาตให้ผู้ดูแลระบบเครือข่าย (Network Manager) สามารถเลือกได้ว่าข้อมูลใดที่จะถูกทำการเข้ารหัสบนเครือข่ายสาธารณะ ส่วนประกอบที่สำคัญของ Metatrust ได้แก่ Digitox ซึ่งเป็นส่วนของข้อมูลที่ถูกเข้ารหัสจากระบบของ RSA และ Interrights Point ซึ่งเป็นส่วน Graphical User Interface (GUI) สำหรับ ผู้ดูแลระบบเครือข่าย (Network Manager) ในการกำหนด Encryption Polycies สำหรับ Digitox

- การสื่อสารความเร็วสูง (Broadband Technology)

เนื่องจากความต้องการในการใช้บริการบน อินเตอร์เน็ต ซึ่งต้องการการสื่อสารด้วยความเร็วสูง (เช่นการดูหนัง online หรือการส่งข้อมูลเพลง online) ในอนาคตอันใกล้จะมีเพิ่มมากขึ้น ดังนั้นผู้ให้บริการการสื่อสารความเร็วสูง จึงคงจะมีส่วนเกี่ยวข้องกับ ไมโครเพย์เมนต์ technology นี้

เทคโนโลยีในอดีตและปัจจุบัน

เทคโนโลยีด้าน ไมโครเพย์เมนต์ ในปัจจุบัน มีทั้งที่สร้างบน hardware (เช่น smartcard) สร้างบน software (เช่น digital wallet) หรือ ทั้งสองอย่างรวมกัน และดังที่กล่าวมาแล้วข้างต้น ทั้ง software และ smartcard ก็มีส่วนในการทำให้การพัฒนาของ ไมโครเพย์เมนต์ เป็นไปอย่างล่าช้า

ปัญหาหลักในการทำ ไมโครเพย์เมนต์ บน software คือ ความสะดวกในการใช้ ส่วนการขาดแคลน infrastructure ที่จะสามารถรองรับ smartcard ก็เป็นปัญหาหลักของการทำ ไมโครเพย์เมนต์บน hardware อย่างไรก็ดี ผู้ผลิต hardware บางรายได้เริ่มนำอุปกรณ์ smart card reader เข้ามาเป็นส่วนประกอบหนึ่งของคอมพิวเตอร์ในบางรุ่น

- ไมโครเพย์เมนต์ บน software

บริษัท IBM และ บริษัท Compaq รวมทั้งบริษัทอื่นๆ กำลังจะทำการออก software สำหรับ ไมโครเพย์เมนต์ ในอนาคตอันใกล้ ผลิตภัณฑ์ software สำหรับ ไมโครเพย์เมนต์ ส่วนใหญ่ จะถูกพัฒนาขึ้นในรูปของ digital wallet (ทำให้สามารถเข้าถึง credit card หรือ ATM card ของผู้ใช้) และ digital certificate โดยชนิดของ digital wallet จะเป็นตัวบ่งบอกถึงวิธีการจ่ายเงินของผู้ใช้ ตัวอย่างเช่น สำหรับผู้ใช้ CyberCash digital wallet เงินจะถูกหักจากบัญชีกระแสรายวันโดย software จากทางผู้ให้บริการ ส่วนผู้ใช้ DigiCash digital wallet จะส่งรหัส 64 bit ไปยังผู้ให้บริการ ซึ่งจะตรวจสอบกับ online bank การใช้ digital wallet มีข้อดีหลายอย่างต่อทั้งผู้ใช้และผู้ให้บริการ รวมทั้งความสะดวกในการใช้จ่าย และความต่อเนื่องในรูปแบบวิธีการจ่าย ส่วนข้อเสียก็ได้แก่การที่ข้อมูลอาจจะรั่วไหลเนื่องจากการให้ข้อมูลบัญชีแก่บาง web site ในขณะนี้หลายๆบริษัทก็ได้ทำการเร่งพัฒนาและออก digital wallet software อื่นๆ เช่น IBM กำลังจะทำการออก Micro-Payment ซึ่ง user จะสามารถจ่ายได้จนถึงอย่างน้อย 1 cent โดยจะใช้ software ซึ่งเป็น browser plugin ทางบริษัท Compaq เองก็จะออกโปรแกรม มิลลิเซ็น ซึ่ง user สามารถใช้ได้จนถึงอย่างน้อย 0.1 cent และสามารถรองรับผู้ใช้หลายๆคนบน wallet อันเดียว

- ไมโครเพย์เมนต์ บน hardware

Smart card เป็นอุปกรณ์เดบิตชนิดหนึ่งซึ่งมีการฝัง microchip ที่รวบรวมข้อมูลการใช้จ่ายเงิน รวมทั้งจำนวนเงินที่สามารถนำไปใช้ได้ อยู่ในการ์ด ข้อดีที่สำคัญอย่างหนึ่งของ Smart card คือ สามารถทำการโอนเงินระหว่างผู้ใช้สองรายได้ อย่างไรก็ตามผู้ที่ต้องการใช้ Smart card จะต้องมีอุปกรณ์ Smart Card reader อยู่ด้วย รวมทั้งความแพร่หลายของระบบ smart card และ infrastructure อย่างที่ได้กล่าวมาแล้วข้างต้น ก็เป็นข้อเสียที่สำคัญของ ไมโครเพย์เมนต์ ระบบนี้

เทคโนโลยีในอนาคต

ในอนาคต เทคโนโลยีอื่นๆ อาจจะถูกนำมารวมกับ ไมโครเพย์เมนต์ technology ในปัจจุบัน เพื่อเพิ่มพูนขีดความสามารถของ ไมโครเพย์เมนต์ เทคโนโลยีที่น่าจะมีส่วนสำคัญคือการพัฒนา server ให้สามารถรองรับจำนวนผู้ใช้ที่เพิ่มขึ้นได้ โดยมีค่าบำรุงรักษาที่ต่ำลง ดังที่ได้กล่าวข้างต้น Unix server มีความสามารถในการรองรับจำนวนผู้ใช้ที่เพิ่มขึ้นได้ดี แต่มีสูง ในขณะที่ NT server มีค่าบำรุงรักษาที่ต่ำแต่ไม่สามารถรองรับผู้ใช้ที่เพิ่มขึ้นได้เป็นอย่างดี การสื่อสารความเร็วสูงซึ่งทำให้สามารถให้บริการเช่น ภาพ และ เสียง บน อินเตอร์เน็ต ก็จะมีส่วนสำคัญในการปฏิวัติการใช้พาณิชย์อิเลคโทรนิคกับไมโครเพย์เมนต์ด้วยเช่นกัน สำหรับทางด้านเทคโนโลยีที่ทำให้การรับส่งเงินแบบอิเล็กโทรนิคนั้น ที่สำคัญคงเป็นการพัฒนามาตรฐานซึ่งทำให้ ไมโครเพย์เมนต์ เป็นที่ยอมรับและแพร่หลาย จากมุมมองทางด้านเทคโนโลยีแล้ว ไมโครเพย์เมนต์ น่าจะมีอนาคตที่สดใส และถ้ารวมการพัฒนาที่เทคโนโลยีต่างๆ ที่จะเกิดขึ้นในอนาคต ไมโครเพย์เมนต์ น่าจะมีส่วนสำคัญในตลาดของ พาณิชย์อิเลคโทรนิกส์ ในอนาคต

2.2 ความปลอดภัยของระบบการสื่อสารข้อมูลผ่านอินเตอร์เน็ต

2.2.1 ความปลอดภัยในเครือข่าย

ในระบบการทำงานบนเครือข่าย การสื่อสารที่เกิดขึ้นระหว่างส่วนต่างๆในระบบจะใช้โปรโตคอลในการสื่อสาร เช่น Transmission Control Protocol / Internet Protocol (TCP/IP) ซึ่งโปรโตคอลต่างๆเหล่านี้สามารถส่งข้อมูลจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งโดยอาศัย สื่อ อุปกรณ์และเครือข่ายคอมพิวเตอร์ ระหว่างทางนี้เป็นการเปิดโอกาสให้บุคคลที่สามสามารถแอบแฝงเข้ามาทำกิจกรรมที่ไม่พึงประสงค์ กรรมวิธีในการดูข้อมูลที่ไหลผ่านระบบเครือข่ายคอมพิวเตอร์นั้นสามารถหาดูได้โดยผู้ที่มีขีดความสามารถ เช่น

- **การดักฟังข้อมูล (Eavesdropping)**

  วิธีนี้ข้อมูลจะยังอยู่เช่นเดิม แต่เนื้อข้อมูลนั้นได้ถูกบุคคลที่สามดักเอาไปใช้งานหรือบันทึกเก็บไว้

- **การดักเปลี่ยนแปลงข้อมูล (Tampering)**

  ข้อมูลจะถูกปรับเปลี่ยนระหว่างทางก่อนที่จะถึงจุดหมาย

- **การแอบอ้างว่าเป็นบุคคลอื่น (Impersonating)**

โดยข้อมูลจะถูกส่งไปที่บุคคลที่แอบอ้างว่าเป็นผู้รับที่ต้องการ หรือในทางกลับกัน ข้อมูลนั้นรับมาจากแหล่งที่แอบอ้างว่าเป็นผู้ส่งที่น่าเชื่อถือ

โดยทั่วไปแล้วผู้ใช้งานในเครือข่ายมักจะไม่เข้าไปยุ่งเกี่ยวหรือแอบดูข้อมูลต่างๆที่วิ่งผ่านเครื่องคอมพิวเตอร์ของตนไป แต่ทว่าข้อมูลบางประเภทซึ่งเป็นความลับและมความสำคัญนั้นมีความจำเป็นที่จะต้องถูกเก็บรักษาไว้อย่างปลอดภัยจากกิจกรรมที่ไม่พึงประสงค์ที่กล่าวมาข้างต้น

จุดหลักที่น่าเป็นห่วงในระบบการทำธุรกรรมทางอินเตอร์เน็ตคือ

- **ความมั่นใจในความเป็นส่วนตัวของข้อมูล (Confidentiality)**

คือระดับความมั่นใจของผู้ทำรายการว่าข้อมูลที่ได้ถูกส่งเข้าไปในระบบของตนจะไม่ถูกผู้ที่ไม่เกี่ยวข้องเข้ามาอ่านได้ เทียบได้กับจดหมายที่ถูกปิดผนึกและไม่มีการฉีกซองโดยผู้ที่ไม่ได้เป็นบุคคลบนจ่าหน้า

- **ความสามารถในการพิสูจน์ตัวจริง (Authentication)**

คือความสามารถในการพิสูจน์ว่าบุคคลที่เข้ามาในระบบ ทั้งผู้ทำรายการและฝ่ายผู้รับรายการ และแม้กระทั่งผู้ที่เกี่ยวข้องกับระบบในส่วนต่างๆ เป็นบุคคลตัวจริงที่สามารถพิสูจน์ได้ มิได้เป็นบุคคลอื่นที่แอบแฝงเข้ามาในระบบ เพื่อให้มั่นใจได้ว่าข้อมูลที่เกิดขึ้นเป็นข้อมูลจริง ที่มิได้เกิดจากการแอบอ้างใดๆ เทียบได้กับการได้เห็นบัตรประจำตัวประชาชน เป็นต้น

- **ความมั่นใจในความสะอาดของข้อมูล (Integrity)**

คือความสามารถในการเกิดความมั่นใจว่า ข้อมูลที่ไหลในระบบมิได้ถูกผู้อื่นบิดเบือนไป คือมิได้มีการถูกสลับเปลี่ยนไประหว่างทาง และเป็นข้อมูลที่ได้มาจากต้นกำเนิด คือผู้กรอกข้อมูลจริงๆ เทียบได้กับการใช้หมึกที่ลบไม่ได้ ไม่มีใครสามารถเปลี่ยนข้อความที่ถูกเขียนโดยหมึกนั้นได้

- **ไม่สามารถปฏิเสธต่อหลักฐานทางข้อมูลได้ (Non-Repudiation)**

ความสามารถในการใช้ข้อมูลรายการที่เกิดขึ้นมาเป็นหลักฐานยืนยันรายการได้ ว่าข้อมูลถูกส่งโดยผู้ที่เป็นผู้ส่งในรายการจริง ถูกรับโดยผู้ที่เป็นผู้รับในรายการจริง ข้อมูลได้เกิดขึ้น ณ เวลาดังกล่าวจริง เป็นต้น ตลอดจนสามารถนำไปใช้เป็นหลักฐานในชั้นศาลได้ เทียบได้กับจดหมายลงทะเบียน หรือการเซ็นรับของ เป็นต้น

การรักษาความปลอดภัยในเครือข่าย

- **การเข้าและถอดรหัสข้อมูล (Encryption and Decryption)**

คือการนำข้อมูลมาเข้ารหัสก่อนที่จะส่งออกไปให้ผู้รับ และผู้รับจะทำการถอดรหัสหลังจากที่ได้รับมา โดยระหว่างที่ข้อมูลเดินทางนั้น ข้อมูลที่เข้ารหัสแล้วจะไม่สามารถอ่านออกได้โดยบุคคลที่สาม

การเข้ารหัสข้อมูล (Encryption) คือกระบวนการรักษาข้อมูลที่เป็นความลับโดยทำการปกปิดข้อมูลเดิมให้อยู่ในรูปที่ไม่สามารถเข้าใจโดยผู้อื่นได้ (Cipher Text) ซึ่งเป็นกลไกในการสื่อสารความลับระหว่างผู้เกี่ยวข้องเท่านั้น ส่วนการถอดรหัส (Decryption) คือขบวนการปรับข้อมูลที่ถูกเข้ารหัสไว้ ให้กลับมาอยู่ในรูปของข้อมูลเดิมที่สามารถเข้าใจได้อีกครั้ง โดยกระบวนการทำการเข้าและถอดรหัส (Cryptographic Algorithm หรือ Cipher) คือฟังก์ชั่นทางคณิตศาสตร์ซึ่งสร้างขึ้นมาเพื่อทำการเข้าและถอดรหัสโดยเฉพาะ

ความสามารถในการเก็บความลับของข้อมูลที่ถูกเข้ารหัสนั้นไม่ได้ขึ้นอยู่กับ Cryptographic Algorithm ซึ่งเป็นที่รู้จักแพร่หลาย แต่จะขึ้นอยู่กับรหัสตัวเลขหรือ กุญแจ (Key) ที่จะต้องนำมาใช้กับ Algorithm เพื่อทำการเข้าหรือถอดรหัส

การเข้ารหัสมีสองแบบ

- **Symmetric Cryptography**

เป็นการเข้ารหัสแบบใช้กุญแจเดียว กระบวนการทาง Symmetric Key cryptography จะมีการประมวลผลที่เร็ว แต่มีจุดที่น่าเป็นห่วงในเรื่องของการแจกจ่ายกุญแจ (key)

รูปที่ 2.2 แสดงการเข้ารหัสข้อความแบบ Symmetric Key

การเข้ารหัสแบบ Symmetric Key นั้นสามารถนำไปใช้ได้อย่างมีประสิทธิภาพ เนื่องจากสามารถนำไปเข้าและถอดรหัสได้อย่างสะดวกและรวดเร็ว และยังสามารถช่วยในการยืนยันตัวบุคคลได้ (Authentication) ในระดับหนึ่ง เพราะการเข้าและถอดรหัสจะใช้แค่ Key เดียวเท่านั้น ไม่สามารถใช้ Key อื่นได้ แต่ทั้งผู้รับและผู้ส่งจะต้องเก็บ Key ไว้เป็นความลับ และไม่เปิดเผยให้ผู้อื่นรู้

- **Public Key Cryptography**

เป็นการเข้ารหัสแบบใช้กุญแจสองตัว ตัวไหนจะเป็นตัวเข้ารหัสก็ได้ อีกตัวจะเป็นตัวที่ใช้ถอดรหัสเสมอ โดยกุญแจทั้งสองตัวที่เกิดขึ้นจะสามารถถูกแจกจ่ายได้หนึ่งตัวเรียกว่า Public Key ส่วนอีกตัวจะต้องเก็บไว้แต่ผู้ที่เป็นเจ้าของ เรียกกุญแจว่า Private Key กระบวนการเข้าและถอดรหัสแบบนี้จะช้ากว่าแบบแรก แต่การบริหารกุญแจทำได้สะดวกกว่า

รูปที่ 2.3 แสดงการเข้าและถอดรหัสข้อความแบบ Asymmetric Key

จากรูป ผู้ส่งข้อมูลทำการเข้ารหัสข้อมูลด้วย Public Key ของผู้รับซึ่งได้แจกจ่ายออกไป และเมื่อผู้รับได้ข้อมูลที่ถูกเข้ารหัสมา จะสามารถถอดออกได้ด้วย Private Key ที่ตนเองเก็บไว้อยู่

เมื่อเปรียบเทียบทั้งสองรูปแบบ การเข้ารหัสแบบ Public Key จะเกี่ยวข้องกับการคำนวณที่ซับซ้อนกว่า ดังนั้นจะไม่ค่อยเหมาะกับปริมาณข้อมูลขนาดใหญ่ แต่สามารถนำมาใช้ในกรณีที่นำเอาการเข้ารหัสแบบ Public Key เพื่อเข้ารหัสตัว Symmetric Key เพื่อเป็นการกระจายตัว Symmetric Key ออกไปได้อย่างปลอดภัย ซึ่งวิธีนี้ถูกนำไปใช้ใน SSL Protocol ดังจะกล่าวในรายละเอียดในหัวข้อถัดไป

2.2.2 หลักการของ Secure Sockets Layer Protocol (SSL) และการแลกเปลี่ยน Certificate

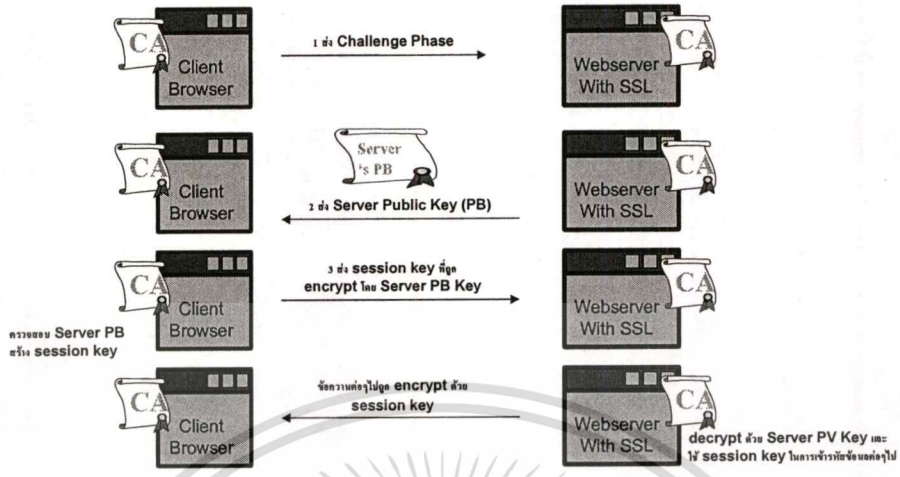
Secure Socket Layer Protocol หรือ SSL นั้นทำงานอยู่บน TCP/IP และอยู่ภายใต้โปรโตคอลที่ทำงานอยู่ระดับ Application Layer เช่น HTTP โดย SSL ใช้งาน TCP/IP แทนโปรโตคอลที่ทำงานอยู่ในระดับบน ซึ่ง SSL จะทำการยืนยัน (Authenticate) Server ที่ใช้ SSL เพื่อติดต่อกับ Client ที่ใช้ SSL ซึ่งทำการยืนยันตัวเองกับ Server เช่นกัน เป็นผลให้สามารถสร้างช่องทางการติดต่อที่มีความปลอดภัยขึ้นมาได้

- **ทำไมจึงต้องมี SSL**

การทำธุรกรรมบนอินเตอร์เน็ตจะไม่ประสบความสำเร็จเลยหากผู้บริโภคไม่มีความมั่นใจในความปลอดภัยของบริการ โดยเฉพาะการนำข้อมูลบัตรเครดิตไปใส่บนหน้าจอเว็บ การใช้ SSL ช่วยให้เกิดความมั่นใจในขั้นตอนการเคลื่อนย้ายของข้อมูล และยังเป็นการยืนยันความน่าเชื่อถือขององค์กรอีกด้วย

- **การทำ SSL Handshake**

โปรโตคอล SSL ใช้เทคนิคของการเข้ารหัสแบบ Public Key และ Symmetric Key มาประยุกต์ใช้เข้าด้วยกัน โดยอาศัยหลักการที่ Symmetric Key นั้นสามารถทำได้รวดเร็วกว่า แต่ Public Key สามารถทำการยืนยันได้ดีกว่า โดยการทำ SSL นั้นจะเริ่มต้นด้วยการแลกเปลี่ยนข้อมูลซึ่งเรียกว่า SSL Handshake ซึ่งเป็นวิธีการยืนยันของทาง Server กับ Client และในทางกลับกันยังสามารถยืนยัน Client กับทาง Server โดยใช้ Public Key หลังจากนั้น Client และ Server จึงร่วมกันสร้าง Symmetric Key เพื่อใช้สำหรับการเข้าและถอดรหัสต่อไป



รูปที่ 2.4 แสดงการทำงานของ SSL โดยการใช้ Asymmetric Key Cryptography มาช่วยในการแลกเปลี่ยน Symmetric Key

- **ความยาวของ Key และความแข็งแรงของการเข้ารหัส**

โดยทั่วไปแล้วความแข็งแรงของการเข้ารหัสขึ้นอยู่กับ ความยากในการค้นพบ Key ที่ใช้เข้ารหัส ซึ่งเกี่ยวเนื่องไปถึง Algorithm และความยาวของ Key ที่ใช้ ดังนั้นความแข็งแรงของการเข้ารหัสมักถูกอธิบายด้วยขนาดความยาวของ Key ที่ใช้ทำการเข้ารหัส กล่าวคือ Key มีความยาวมาก ความแข็งแรงในการเข้ารหัสก็มีมากด้วย โดยการวัดขนาดของ Key นั้นมีหน่วยเป็น บิต (Bits) ยกตัวอย่างเช่น 128-bit key ที่ใช้ใน RC4 Symmetric Key ซึ่งใช้เข้ารหัสใน SSL นั้นมีความปลอดภัยสูงกว่า 40-bit key ใน Algorithm เดียวกันมาก กล่าวคือ การเข้ารหัสด้วย 128-bit RC4 นั้นมีความแข็งแรงกว่าแบบ 40-bit key ถึง 3×10^{26} เท่า

- **ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate)**

ใบรับรองอิเล็กทรอนิกส์ คือ เอกสารทางอิเล็กทรอนิกส์ที่ใช้ระบุและยืนยันบุคคล server บริษัท หรือ สิ่งอื่นๆ โดยอิงกับ Public Key ของบุคคลหรือสิ่งนั้น ซึ่งกลไกการทำ Public Key จะอาศัยใบรับรองอิเล็กทรอนิกส์ ใช้แก้ปัญหาของการปลอมแปลงหรอแอบอ้างเป็นบุคคลอื่น (Impersonation)

โดยการใช้งานใบรับรองอิเล็กทรอนิกส์ จะมีรูปแบบการใช้งานเหมือนเอกสารทั่วไป เช่น บัตรประจำตัวประชาชน ใบขับขี่ เป็นต้น สำหรับใบรับรองอิเล็กทรอนิกส์ จะมี Certificate Authority (CA) ซึ่งมีหน้าที่ออกใบรับรองให้กับบุคคลหรือสิ่งที่ผ่านการตรวจสอบ และยืนยันเป็นที่เรียบร้อยแล้ว โดย CA นั้นอาจเป็นองค์กรอิสระที่ทำหน้าที่ของ CA (Trusted Third Party CA) หรือเป็น CA ระดับองค์กร (Enterprise CA)

ใบรับรองอิเล็กทรอนิกส์ที่ CA ออกให้นั้นจะทำการผูก Public Key เข้ากับชื่อของสิ่งที่ต้องการยืนยัน เช่น ชื่อของบุคคล หรือ ชื่อของ server เป็นต้น

- **รูปแบบการยืนยันตัวบุคคล (Forms of Authentication)**

การยืนยันตัวบุคคล (Authentication) เป็นกระบวนการตรวจสอบเพื่อยืนยันบุคคล หรือสิ่งต่างๆ แบ่งเป็น

การยืนยันผู้เข้าใช้บริการ (Client Authentication) คือยืนยันตัวบุคคลผู้ขอใช้บริการกับทาง Server

การยืนยันผู้ให้บริการ (Server Authentication) คือยืนยันถึงผู้ให้บริการหรือเครื่อง Server ที่ผู้ใช้บริการติดต่อ

- **การยืนยันตัวบุคคลโดยใช้ใบรับรองอิเล็กทรอนิกส์ (Certificate Based Authentication)**

วิธีการยืนยันของผู้เข้าใช้บริการ ด้วยการใช้ใบรับรองอิเล็กทรอนิกส์นั้นเป็นส่วนหนึ่งของกลไกการทำโปรโตคอล SSL คล่าวคือทางผู้ใช้บริการจะทำการลงลายเซ็นอิเล็กทรอนิกส์กับข้อมูลที่สุ่มขึ้นมา และ ส่งใบรับรองอิเล็กทรอนิกส์มากับข้อมูลที่ลงลายเซ็นแล้ว ผ่านเครือข่ายมายัง Server ซึ่งใช้กระบวนการถอดรหัสแบบ Public Key Cryptography เพื่อทำการตรวจสอบลายเซ็น และ ใบรับรองอิเล็กทรอนิกส์ ที่ส่งมา

- **Certificate Authority**

Certificate Authority มีหน้าออกใบรับรองอิเล็กทรอนิกส์ให้กับบุคคล หรือสิ่งที่ผ่านการตรวจสอบ และ ยืนยันหลักฐานเป็นที่เรียบร้อยแล้ว โดย CA มีได้หลายแบบ ดังนี้

CA เพื่อการพาณิชย์ (Commercial CA หรือ Trusted Third Party CA) คือ CA ที่จัดตั้งขึ้นเพื่อเป็นบุคคลกลางทำหน้าที่ในการยืนยันบุคคล บริษัท หรือ สิ่งนั้นๆ ที่ต้องการยืนยัน โดยอิงกับ Public Key ของบุคคลนั้นๆ และออกใบรับรองอิเล็กทรอนิกส์เพื่อพิสูจน์ว่าบุคคลนั้นๆ เป็นตัวจริง และเป็นเจ้าของ Public Key ที่ระบุไว้ในใบรับรองอิเล็กทรอนิกส์

ลักษณะนี้จะใช้ออกสำหรับผู้ใช้ในระดับกว้าง เนื่องจากลักษณะเครือข่ายมีขนาดใหญ่และมีผู้ใช้งานเป็นจำนวนมากซึ่งต้องการบุคคลกลางที่น่าเชื่อถือเข้ามารับรอง

CA ในระดับองค์กร (Enterprise CA หรือ Organiztion CA) คือ CA ที่จัดตั้งขึ้นเพื่อตอบสนองความต้องการในระดับองค์กรในการใบรับรองอิเล็กทรอนิกส์ เพื่อจัดการผู้ใช้งานที่ต้องการติดต่อและใช้งานระบบ

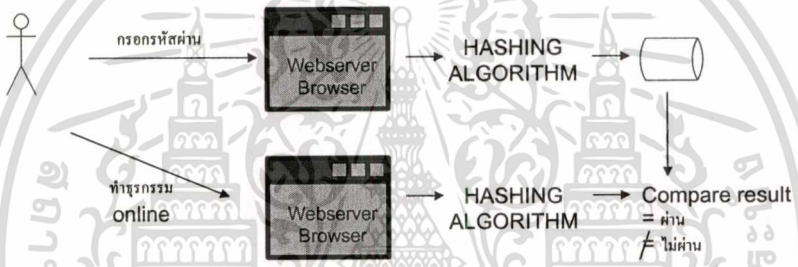
2.2.3 ความปลอดภัยของตัวข้อมูลบนระบบแอพลิเคชั่นที่ใช้งานบนอินเตอร์เน็ต

นอกจากการคำนึงถึงความปลอดภัยของข้อมูลที่วิ่งบนอินเตอร์เน็ตแล้ว การเก็บรักษาข้อมูลบนฐานข้อมูลในระบบก็มีความสำคัญเช่นกัน การเก็บข้อมูลในฐานข้อมูลสามารถมีการเข้ารหัสข้อมูลก่อนที่จะนำลงสู่ฐานข้อมูล เพื่อกันไม่ให้ผู้ที่มีสิทธิในการเข้าใช้ฐานข้อมูลสามารถอ่านข้อมูลออก โดยมากในการพัฒนาระบบ มักจะแยกบุคคลที่รู้กรรมวิธีในการถอดรหัสข้อมูลมาสู้ข้อมูลดั้งเดิม กับ ผู้ที่มีสิทธิในการเข้าดึงข้อมูล ออกจากกัน เพื่อความปลอดภัยของข้อมูล

กรรมวิธีต่างๆที่สามารถนำมาใช้ในการเก็บข้อมูลในฐานข้อมูล เช่น การเข้ารหัสข้อมูลก่อน คือแบบ Encryption ไม่ว่าจะเป็นแบบ Symmetric Key หรือ Asymmetric Key โดยถ้าเป็น Symmetric Key ก็จะต้องคำนึงถึงวิธีการเก็บรักษา Key ด้วย ส่วน Asymmetric Key ก็จะต้องคำนึงถึงวิธีการเก็บรักษาทั้ง Private Key และ Public Key โดยคำนึงเสมอว่า Private Key จะไม่สามารถให้ใครรู้ได้

อีกวิธีในการปกปิดข้อมูลคือการทำการย่อยข้อมูล (Hashing) การทำการ Hash นั้นเป็นฟังค์ชั่นทางคณิตศาสตร์ที่ทำการแปลงข้อมูลไปสู่อีกรูปแบบหนึ่ง โดยเป็นการแปลงทางเดียว กล่าวคือไม่สามารถแปลงกลับได้ ซึ่งตรงจุดนี้จะต่างจากการเข้าและถอดรหัสทั่วไป เรียกอีกแบบว่า One Way Hash หรือ Message Digest นั่นเอง

การทำ Hash กับข้อมูลเดิมจะได้ผลลัพธ์เดิมเสมอ ดังนั้นกับข้อมูลบนฐานข้อมูล โดยมากจะทำกับข้อมูลที่ไม่จำเป็นต้องมีการแปลงกลับ และเป็นข้อมูลที่ต้องการความปลอดภัย และมักทำเพื่อเป็นการพิสูจน์ความถูกต้องของข้อมูล เช่น การตรวจสอบรหัสผ่าน (Password) โดยสามารถนำรหัสผ่านมาทำการ Hashing ด้วย Hashing Algorithm ก่อนจากนั้นนำไปเก็บในฐานข้อมูล ณ จุดนี้ ผู้ที่ไม่รู้รหัสผ่าน และถึงแม้จะมีตัว Hashing Algorithm อยู่ในมือก็ไม่สามารถคาดเดาได้ว่ารหัสผ่านคืออะไร จากนั้นเมื่อ user กรอกรหัสผ่านเข้ามาในระบบ จึงทำการ Hashing อีกครั้งและนำไปเทียบกับค่าในฐานข้อมูล หากค่าตรงกันถือว่า รหัสผ่านถูกต้อง ทั้งนี้การทำ Hashing Algorithm กับข้อมูลคนละตัวจะไม่มีทางได้ผลลัพธ์เป็นตัวเดียวกัน



รูปที่ 2.5 แสดงการพิสูจน์รหัสผ่านโดยใช้กรรมวิธีของ Hashing

2.3 หลักการของการพัฒนาเว็บแอพลิเคชั่นโดยใช้ PHP บน Window และ IIS Web Server

PHP จัดเป็น Server-side Script ซึ่งสามารถทำงานในลักษณะ

- ทำงานแบบ Server-side Script เป็นที่นิยมที่สุด ซึ่งต้องการส่วนประกอบสามส่วนในการทำงาน ลักษณะนี้คือ PHP Parser (CGI หรือ Server Module) และ Webserver และ Web Browser ในการทำงานลักษณะนี้จะต้อง run Webserver ที่มี PHP ติดตั้งไว้แล้ว และสามารถดูผลการทำงานของ PHP ได้ผ่าน Web Browser
- แบบ Command Line Script สามารถ run PHP โดยไม่มี Server หรือ Browser ก็ได้ แค่เพียงมี PHP Parser เท่านั้น การทำงานลักษณะนี้เหมาะกับการทำงานพวก Script programming task บน Unix ทั่วไป หรือ Task Scheduler บน Windows ก็ได้

PHP สามารถถูกเรียกใช้งานได้บนระบบปฏิบัติการหลักๆได้เกือบทุกตัว อาทิเช่น Linux, Unix (HP-UX, Solaris and OpenBSD), Microsoft Windows, Mac OS X, RISC OS, และอื่นๆ และ PHP ยังสามารถทำงาน

ร่วมกับ Webserver ต่างๆ ได้หลายตัวเช่นกัน อาทิเช่น Apache, Microsoft Internet Information Server, Personal Web Server, Netscape and iPlanet servers, Oreilly Website Pro server, Caudium, Xitami, OmniHTTPd, และอื่นๆ

ดังนั้นจะเห็นได้ว่าการเลือกใช้ PHP เป็นการสะดวกต่อผู้พัฒนาที่สามารถนำ Source Code ย้ายไปใส่ Platform อื่นได้ในอนาคต ทำให้ระบบไม่ยึดติดกับ Platform ฝั่ง Server

PHP มีความสามารถในการแสดงผล HTML รูปภาพ พล็อตกราฟ ไฟล์ PDF และแม้กระทั่ง ไฟล์ Flash และความสามารถในการสร้าง XML หรือแม้กระทั่งสร้าง Server-side Cache ให้กับระบบได้

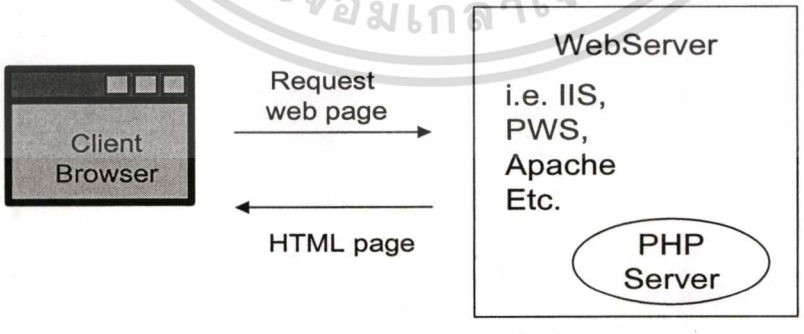
จุดที่น่าสนใจของ PHP คือสามารถทำให้เป็น Dynamic Content ได้อย่างสมบูรณ์แบบ และความสามารถในการสร้างส่วน CGI Programming ออกจากการสร้างหน้าจอด้วย HTML Tag ที่เรียกว่า Template ทำให้ผู้พัฒนาระบบสามารถ Maintain ระบบได้อย่างมีประสิทธิภาพ

จุดที่น่าสนใจอีกส่วนและเด่นที่สุดของ PHP คือความสามารถในการทำงานร่วมกับ Database ได้หลากหลาย ทำให้ผู้พัฒนาระบบสามารถเปลี่ยนแปลงระบบฐานข้อมูลในภายหลังได้สะดวก ดังนั้นการพัฒนาเว็บที่มีส่วนของฐานข้อมูลเข้ามาเกี่ยวจึงเป็นเรื่องที่สะดวก

ปัจจุบัน PHP สามารถทำงานร่วมกันกับระบบฐานข้อมูลต่อไปนี้

Adabas D	Ingres	Oracle (OCI7 and OCI8)
dBase	InterBase	Ovrimos
Empress	FrontBase	PostgreSQL
FilePro (read-only)	mSQL	Solid
Hyperwave	Direct MS-SQL	Sybase
IBM DB2	MySQL	Velocis
Informix	ODBC	Unix dbm

และ PHP ยังสนับสนุนการใช้งาน ODBC ร่วมกับระบบฐานข้อมูลต่างๆ สำหรับการทำงานของระบบเว็บแอพลิเคชั่นที่มี PHP เป็น Server-Side Script มีหน้าตาดังนี้



รูปที่ 2.6 แสดงการทำงานของแอพลิเคชั่นที่ใช้ PHP

บทที่ 3

การออกแบบและพัฒนาระบบ

3.1 การออกแบบข้อกำหนดของระบบ

3.1.1 ข้อกำหนดของระบบงานมีดังนี้

- ผู้ให้บริการสามารถให้บริการได้หลายร้านค้าในเวลาเดียวกัน
- ร้านค้าสามารถมี user ที่เข้ามาตรวจสอบข้อมูลต่างๆภายในเว็บผู้ให้บริการได้หลายระดับ
- ทุกรายการที่ส่งเข้ามาจากร้านค้าจะต้องทำการชำระได้สำเร็จหากลูกค้ามีตัวตนจริง
- ลูกค้าจะต้องซื้อ e money โดยชำระผ่านบัตรเครดิตแบบออนไลน์
- ลูกค้าจะมี e money (คูปอง) ครั้งละ 1 ใบ และสามารถเติมเงินได้ทุกครั้งที่ต้องการ
- e money (คูปอง) แต่ละใบจะมีการจำกัดอายุการใช้งาน
- ลูกค้าสามารถเข้ามาตรวจสอบประวัติการชำระ e money (คูปอง)ได้
- ลูกค้าสามารถเข้ามาตรวจสอบประวัติการเติมเงินใส่ e money (คูปอง)ได้
- ต้องไม่มีการชำระซ้ำ
- ต้องไม่มีการปลอมแปลงการทำรายการได้
- รายการชำระเงินถูกทำโดยเจ้าของเงินเท่านั้น
- การผลิตเงินจะต้องมีประสิทธิภาพและถูกต้อง

3.1.2 การออกแบบการดำเนินงานทางธุรกิจในระบบ

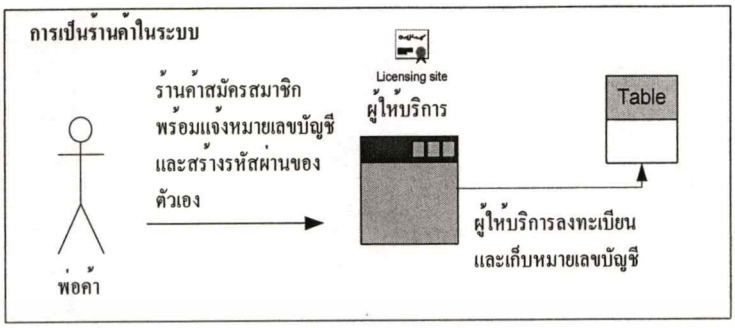
ระบบการทำงานจะต้องมีส่วนของระบบไมโครเพย์เมนต์ก่อน โดยระบบโครงสร้างหลักจะประกอบไปด้วย ระบบฝั่งผู้ให้บริการ และระบบฝั่งร้านค้าสมาชิก

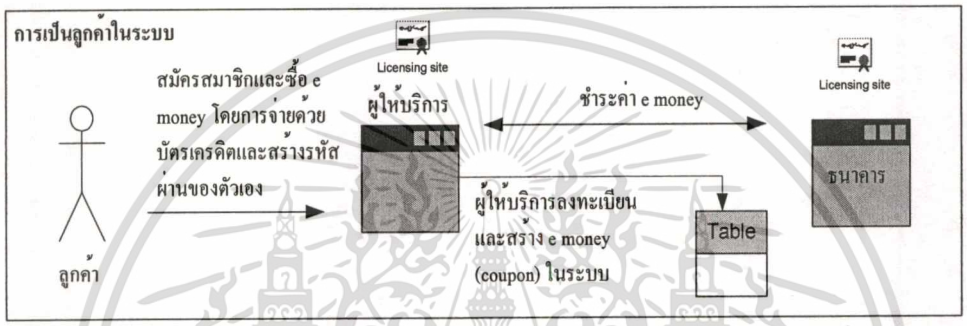
1. **ระบบฝั่งผู้ให้บริการจะต้องประกอบไปด้วย**
    - ส่วนการรับร้านค้าสมาชิกใหม่ (Merchant Registration)
    - ส่วนการบริหารผู้ใช้งานของร้านค้า (Merchant User Management)

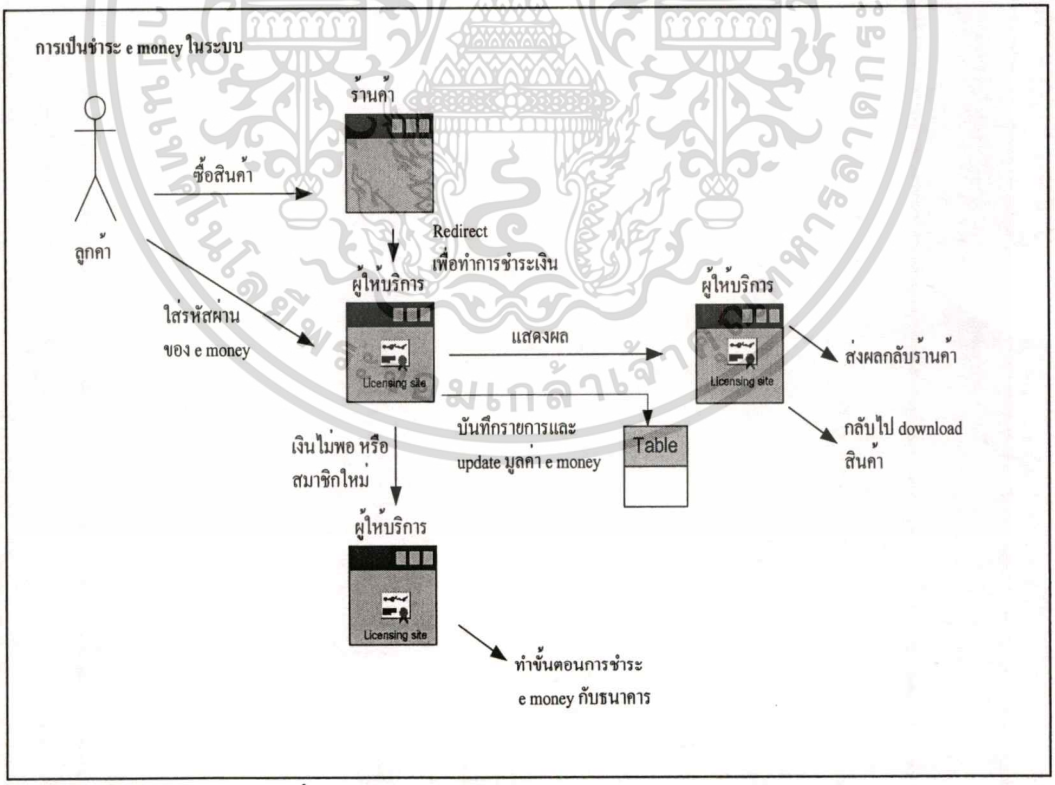
- ส่วนการเปลี่ยนรหัสผ่านเข้าสู่ระบบ (Merchant Password Management)
- ส่วนการตรวจดูรายงานของผลประกอบการและเบิกจ่ายเงิน (Merchant Account Management)
- ส่วนของการดูรายการของธุรกรรมที่เกิดขึ้นในระบบได้แบบออนไลน์ (Merchant Transaction Report)
- ส่วนการขายเงินอิเล็กทรอนิกส์ (e money Purchasing)
- ส่วนการให้ลูกค้าเข้ามาตรวจสอบรายการของ e money ที่ได้ซื้อไปที่เกิดขึ้นในระบบได้ (e money Transaction)
- ส่วนสมัครสมาชิกใหม่ (New Registration)
- ส่วนการต่อเชื่อมกับธนาคารเพื่อทำการชำระค่า e money ซึ่งมีการทำเป็นแบบ macro payment โดยใช้บัตรเครดิตของลูกค้า (e money Purchasing Payment)
- ส่วนการเติมเงินให้กับ e money (e money Refill)
- ส่วนการบริหารรหัสผ่านของลูกค้า (Customer Password Management)
- ส่วนการบริหารรหัสที่ใช้คู่กับ e money (e money Passcode Management)
- ส่วนการรับชำระรายการออนไลน์ (Online Micropayment)
- ส่วนการแสดงผลการชำระรายการออนไลน์ (Payment Result)
- ส่วนการแจ้งการใกล้หมดอายุของ e money (e money Expire Alerting)
- ส่วนการรับการตอบรับการต่ออายุ (e money Expiry Extension Management)

2. ระบบฝั่งร้านค้าจะต้องประกอบไปด้วยการเตรียมการในส่วน
   - ส่วนการขายสินค้า (Store)
   - ส่วนการเชื่อมต่อกับผู้ให้บริการ (Connect to Broker for Transaction)
   - ส่วนการรับผลการชำระมูลค่าสินค้า (Receive Transaction Result)

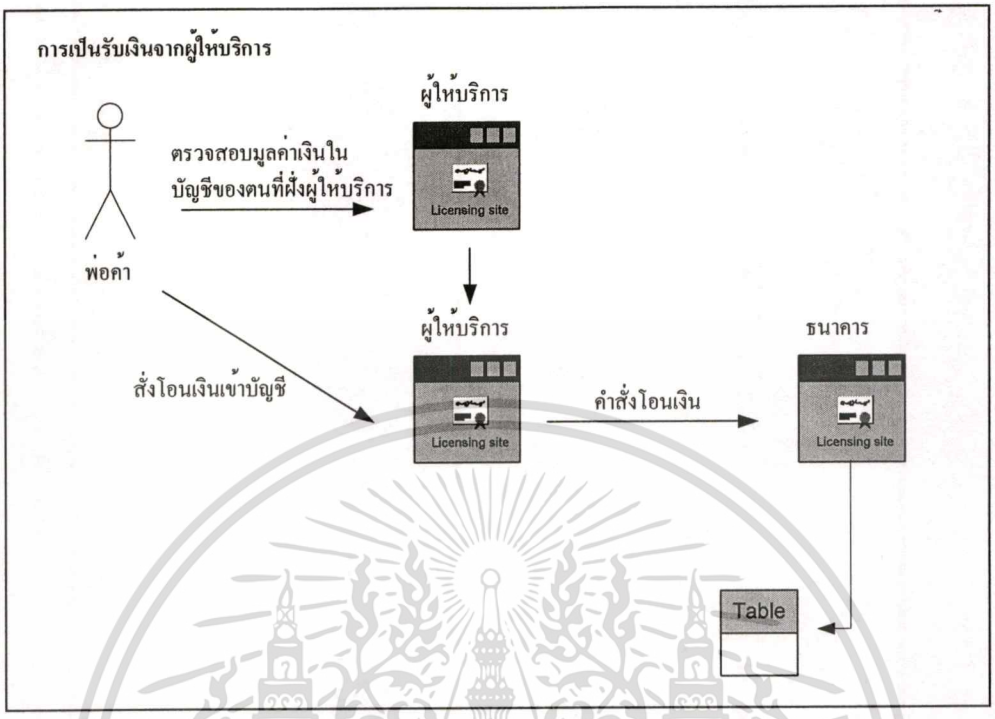
เมื่อมีโครงสร้างหลักแล้ว ระบบสามารถเปิดให้บริการกับผู้บริโภคที่ต้องการจะเข้ามาสมัครเป็นสมาชิกของระบบ และเข้ามาซื้อเงินอิเล็กทรอนิกส์ (e money) ได้







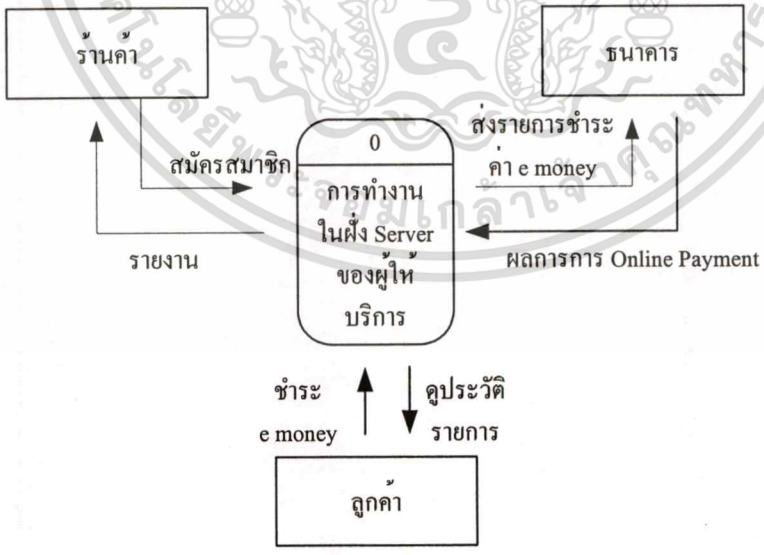
รูปที่ 3.1 แสดงการไหลของการดำเนินงานทางธุรกิจ



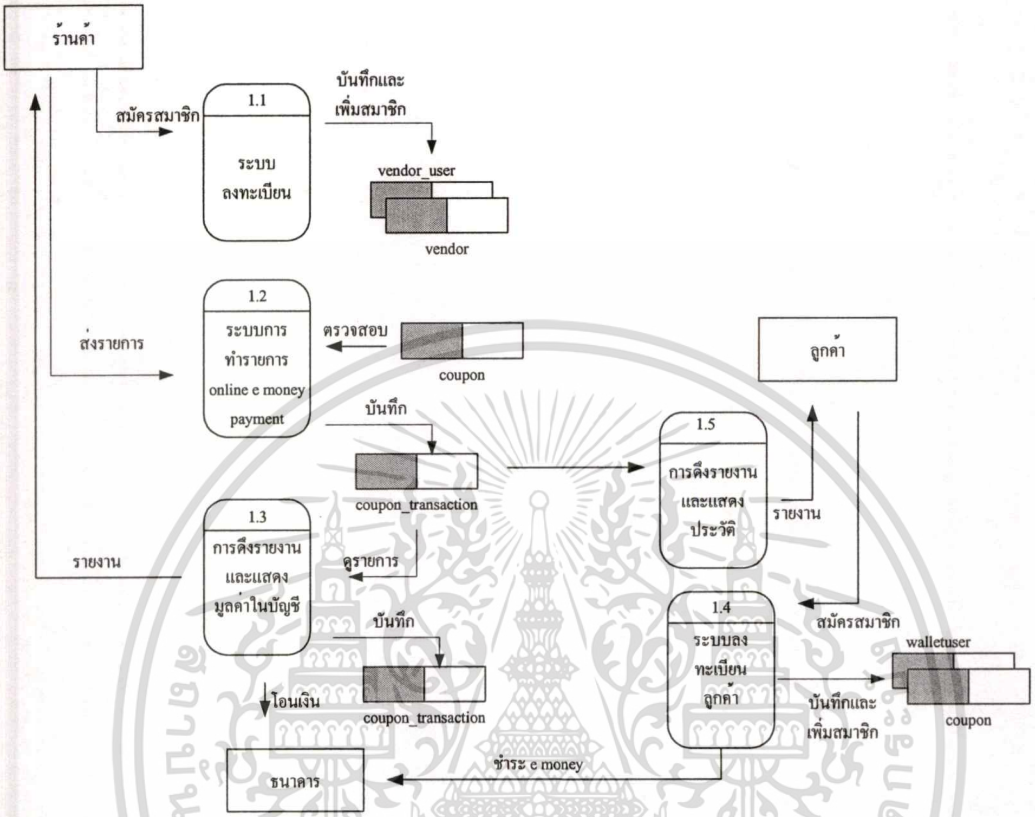
รูปที่ 3.2 แสดงการไหลของการดำเนินงานทางธุรกิจ (ต่อ)

3.2 การออกแบบการทำงานของหน่วยงานต่างๆในระบบ

3.2.1 การทำงานในฝั่ง server ของผู้ให้บริการ

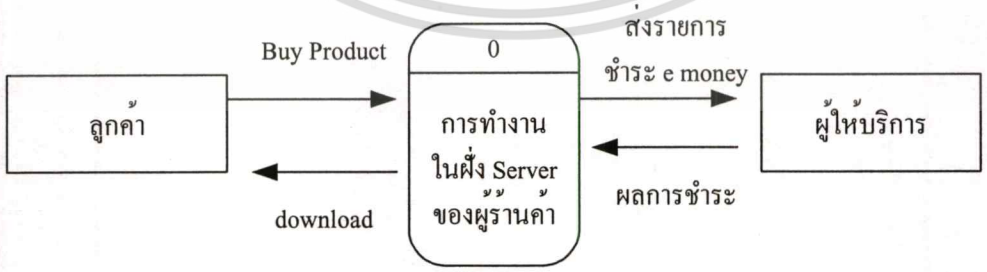


รูปที่ 3.3 Context Diagram ของฝั่ง Server ผู้ให้บริการ

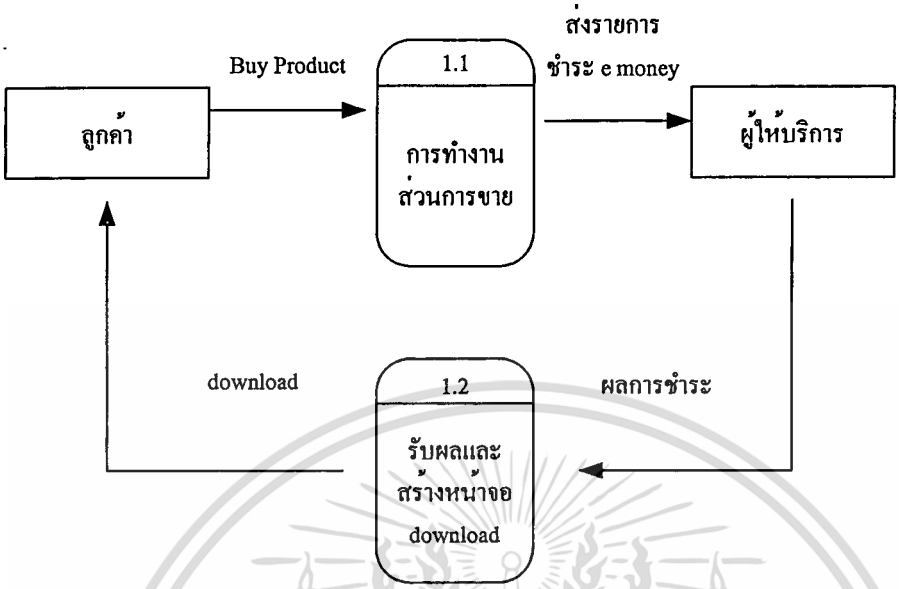


รูปที่ 3.4 Diagram 1 DFD ของฝั่ง Server ผู้ให้บริการ

3.2.2 การทำงานในฝั่ง server ของร้านค้า

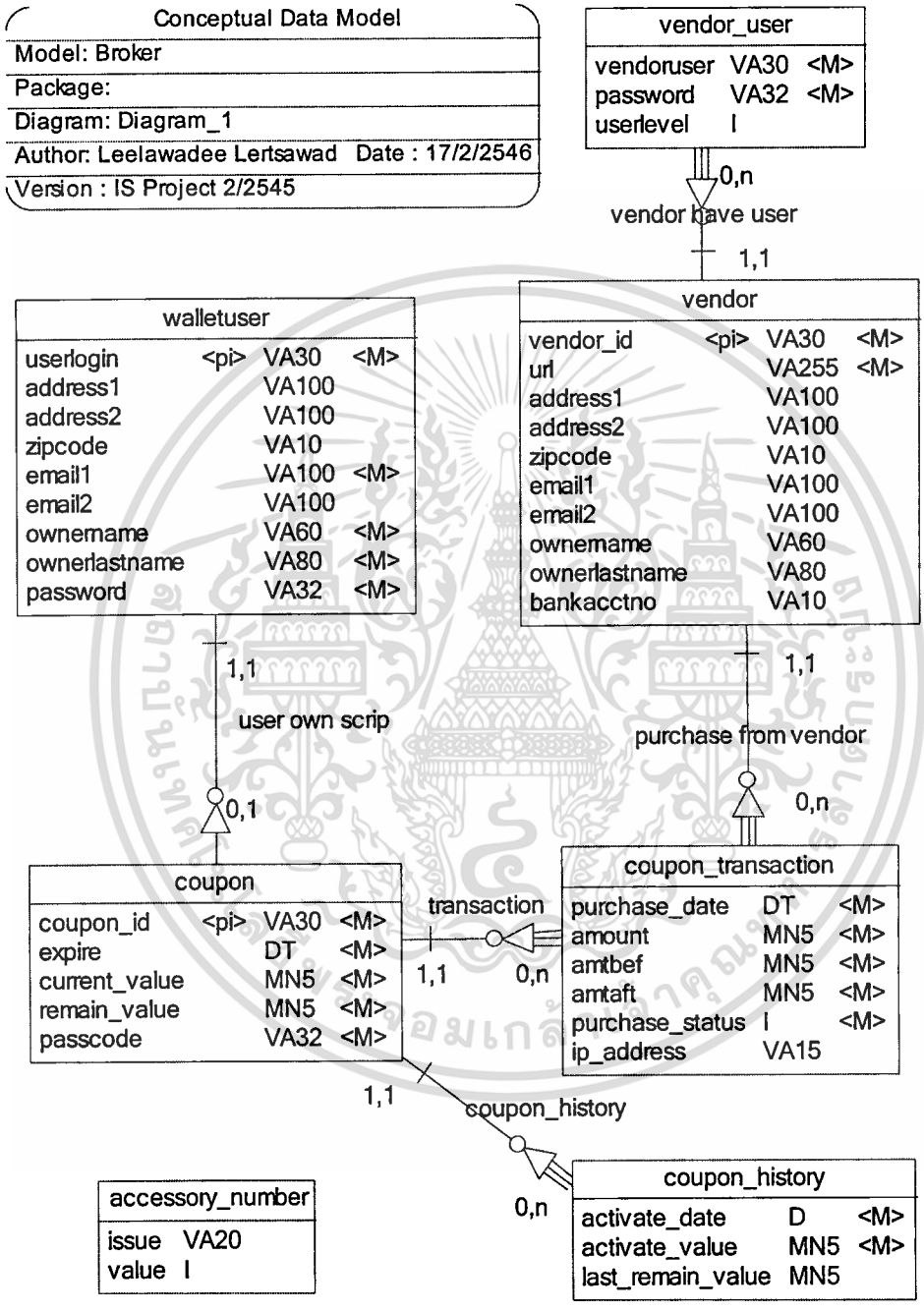


รูปที่ 3.5 Context Diagram ของฝั่ง ร้านค้า

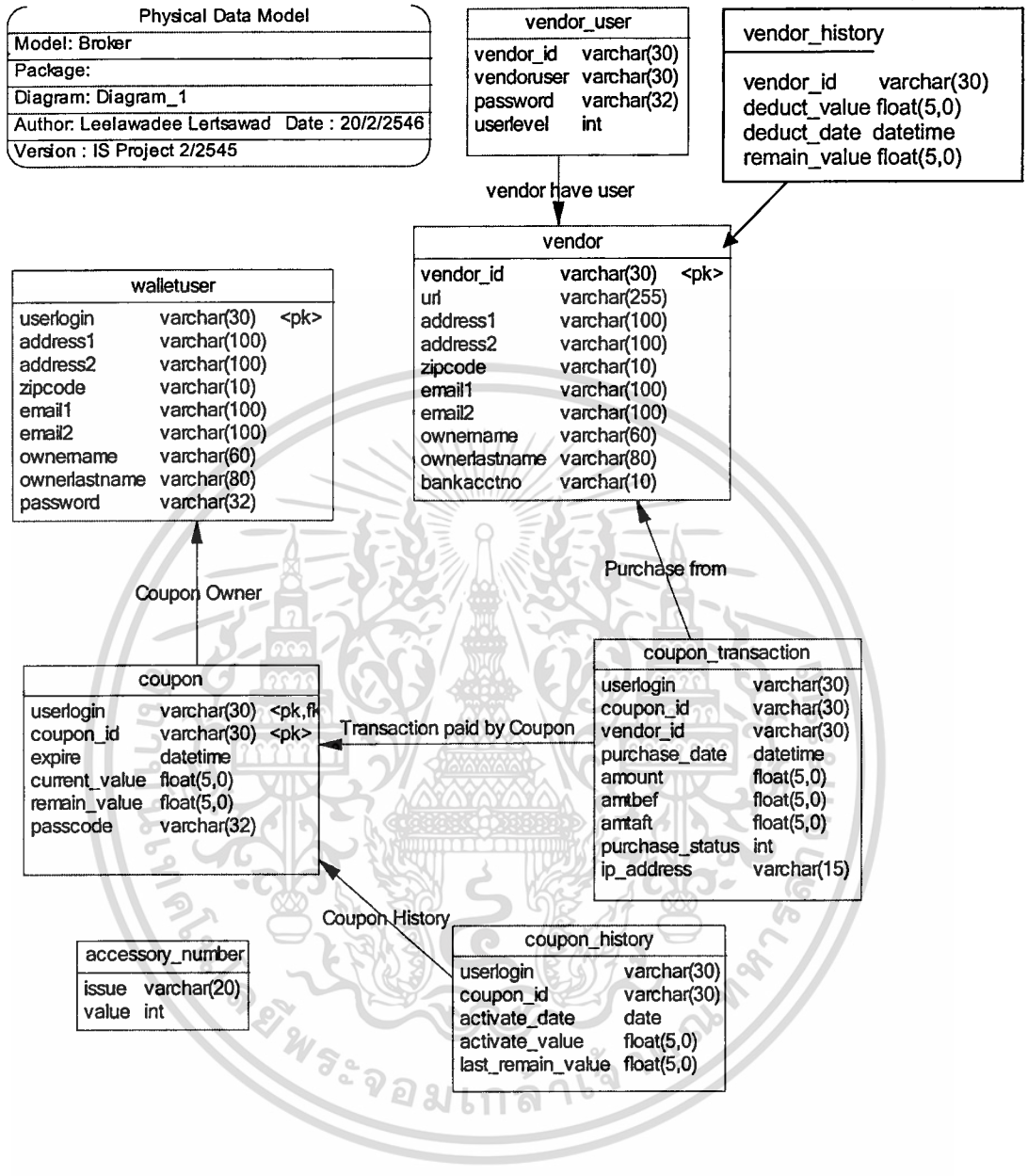


รูปที่ 3.6 Diagram 1 DFD ของฝั่ง ร้านค้า

3.3 การออกแบบระบบฐานข้อมูล



รูปที่ 3.7 แสดง Conceptual Data Model ของระบบฐานข้อมูลฝั่ง Server ผู้ให้บริการ



รูปที่ 3.8 แสดง Physical Data Model ของระบบฐานข้อมูลฝั่ง Server ผู้ให้บริการ

- **รายละเอียดของฐานข้อมูล**

รหัสผ่าน (Password) ของลูกค้าในระบบจะถูกเก็บไว้ที่ walletuser Table ส่วนรหัสผ่าน (Password) ของ User ของร้านค้าในระบบจะถูกเก็บไว้ที่ vendor_user Table

โดยข้อมูลรหัสผ่านจะมีกระบวนการเก็บที่เหมือนกันคือ มีการ hashing ของข้อมูลก่อนการเก็บ โดย function ที่ใช้ในการ Hashing มีการ Coding ดังนี้

```
function hmac ($key,$data)
{
    $b=64; //byte length for md5
    if (strlen($key) > $b) {
            $key=pack("H*",md5($key));
    }
    $key = str_pad($key, $b, chr(0x00));
    $ipad = str_pad('',$b, chr(0x36));
    $opad = str_pad('',$b, chr(0x5c));
    $k_ipad = $key ^ $ipad;
    $k_opad = $key ^ $opad;

    return md5($k_opad . pack("H*",md5($k_ipad.$data)));
}//end hmac
```

ส่วนประกอบที่สำคัญในระบบอีกจุดคือ e money ซึ่งเมื่อถูกสร้างขึ้นมาจะเก็บอยู่ในตาราง coupon ซึ่งมี Data Item ดังนี้

- walletuser.userlogin คือ userlogin ที่ลูกค้าใช้ login เข้าระบบ และแสดงความเป็นเจ้าของ e money โดยในระบบออกแบบให้ 1 userlogin มี e money (coupon) ได้เพียง 1 อัน
- coupon.coupon_id เป็น Primary ร่วมกับ userlogin ในตาราง
- coupon.expire วันเวลาที่ coupon_id นี้จะหมดอายุ
- coupon.current_value มูลค่าของ coupon_id นี้ตอน ณ ขณะใดขณะหนึ่ง เป็นมูลค่าที่เป็นเงินจริง
- coupon.remain_value มูลค่าของ coupon_id นี้ที่คงเหลือ ณ ปัจจุบันเป็นมูลค่าที่หักตามรายการที่มาขอตรวจสอบยอดหรือเรียกว่ารายการที่ยังไม่ได้ดาวน์โหลดด้วย

ยกตัวอย่าง

1. *current_value เป็น 1000 บาท มีรายการเข้ามา 20 บาท*
2. *เมื่อระบบตรวจสอบแล้วว่า passcode ถูกต้องและมูลค่า remain_value มีเพียงพอ ก็จะตัดยอด remain_value ลงไป 20 บาทสมมุติให้ remain_value มีอยู่ 800 บาท ดังนั้นจะเหลือ 780 บาทและยังคงเป็น 1000 บาท*
3. *เมื่อร้านค้าได้ผลลัพธ์และส่ง activate มาบอกว่าลูกค้าได้ดาวน์โหลดแล้วระบบจะปรับ current_value-amount=1000-20=980 และ remain_value ยังเท่าเดิม*

- passcode รหัสผ่านสำหรับจ่าย coupon_id นี้ ลูกค้าสามารถตั้งเป็นค่าเดียวกันกับ password ของการ login ได้
- coupon_transaction.purchase_status มี 2 state คือ

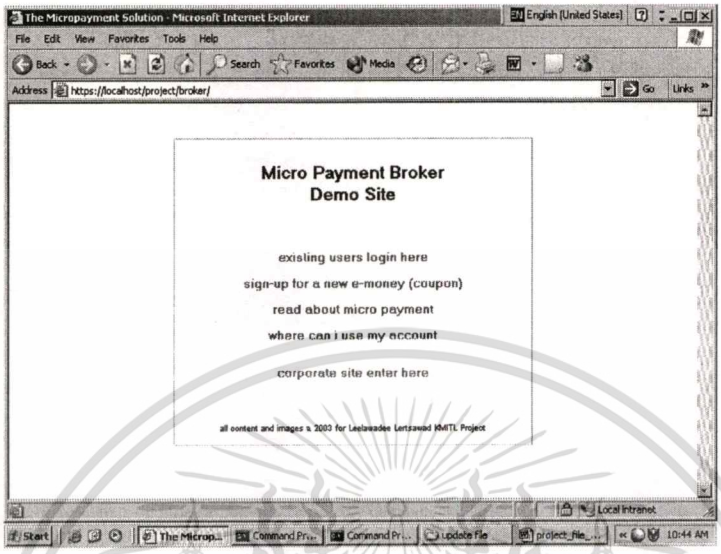
  1 'wait for response'

  2 'deducted' (from coupon.current_value and product downloaded)

รายละเอียดตารางในระบบผู้ให้บริการ (Broker)

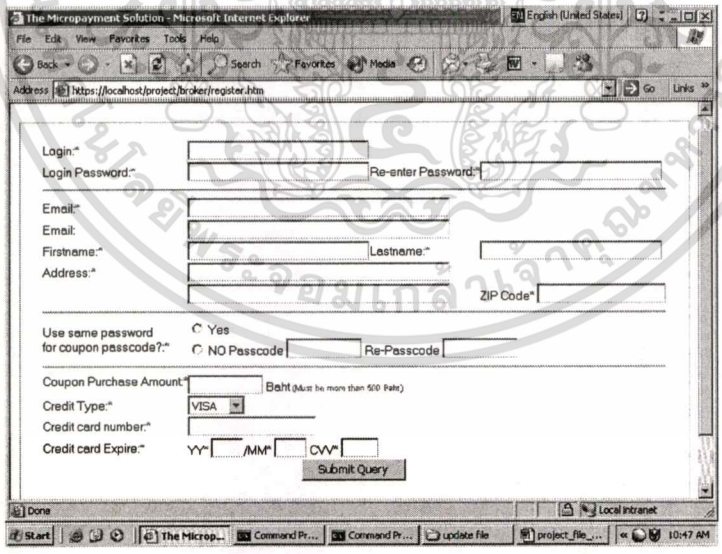
- walletuser เก็บข้อมูลเจ้าของ coupon
- vendor เก็บข้อมูลร้านสมาชิก
- vendor_user เก็บข้อมูลรหัสผ่านของผู้ดูแลระบบของร้านค้า
- vendor_history เก็บประวัติการเบิกจ่ายเงินจากระบบ
- accessory_number เก็บเลข running number ไว้ใช้ในระบบ
- coupon_history เก็บประวัติการเติมเงิน
- coupon_transaction เก็บรายการของ coupon
- coupon เก็บข้อมูลของ coupon (ie. expire, value, password etc.)

3.4 การออกแบบหน้าจอ



รูปที่ 3.9 แสดงหน้าจอหลักของผู้ให้บริการ

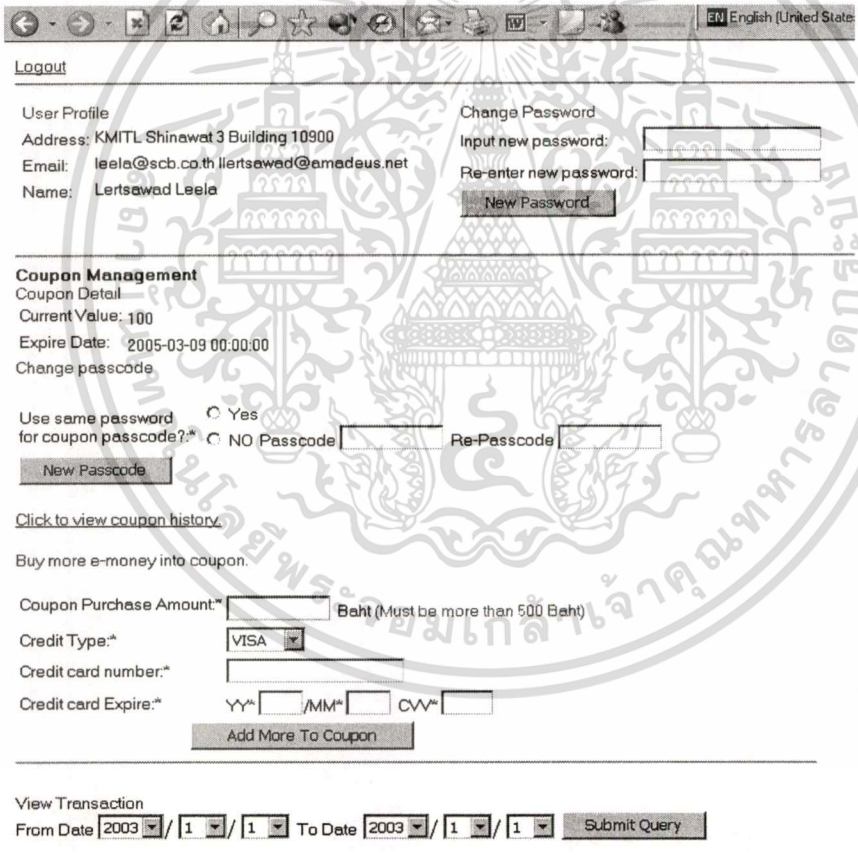
เมื่อลูกค้าสมัครเป็นสมาชิกครั้งแรกต้องกรอกส่วน Sign up for new e-money จากนั้นจะไปยัง รูป 3.10



รูปที่ 3.10 แสดงหน้าจอการซื้อ e money (coupon) ครั้งแรก

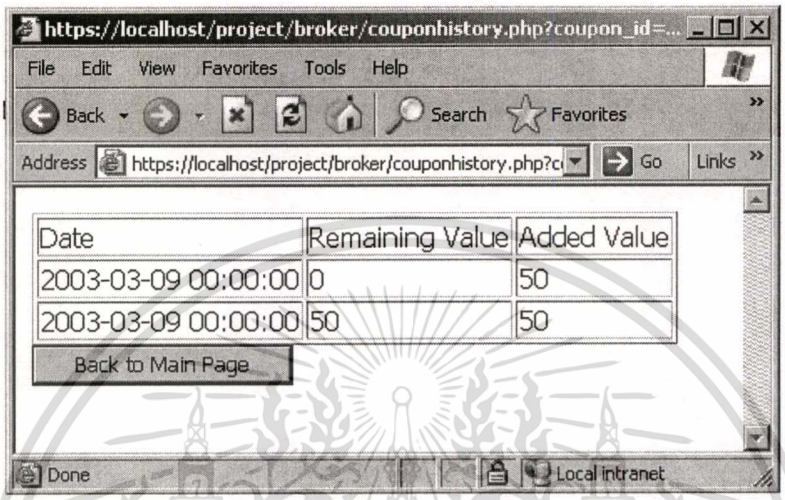
จากนั้นจากหน้าจอหลักไปที่ existing users login here

รูปที่ 3.12 แสดงหน้าจอการ login เข้าไประบบของลูกค้า



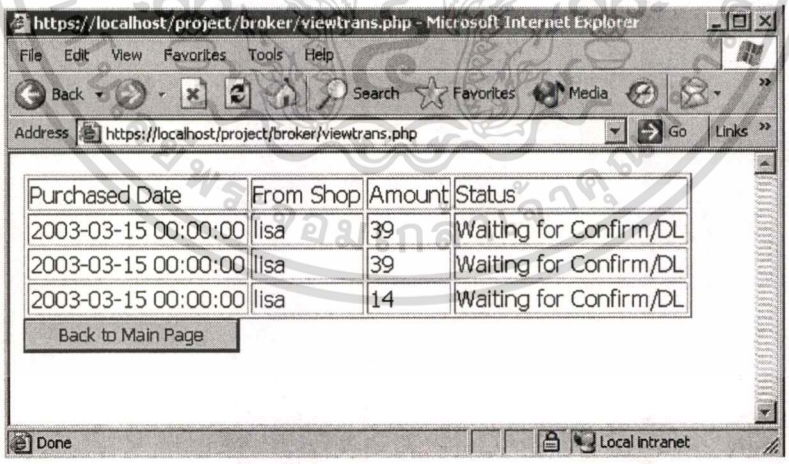
รูปที่ 3.13 แสดงหน้าจอการ เข้าไปดู Wallet และ Manage User Wallet ของลูกค้า

ในหน้าจอนี้ เป็นหน้าจอหลักสำหรับการ Login ของลูกค้า ลูกค้าสามารถ ตรวจสอบดูประวัติการซื้อและชำระรายการ e money ของตนได้ และสามารถเพิ่มมูลค่าใน e money ได้ ตลอดจนเปลี่ยนรหัสผ่านของ e money และเปลี่ยนรหัสผ่านของการ login

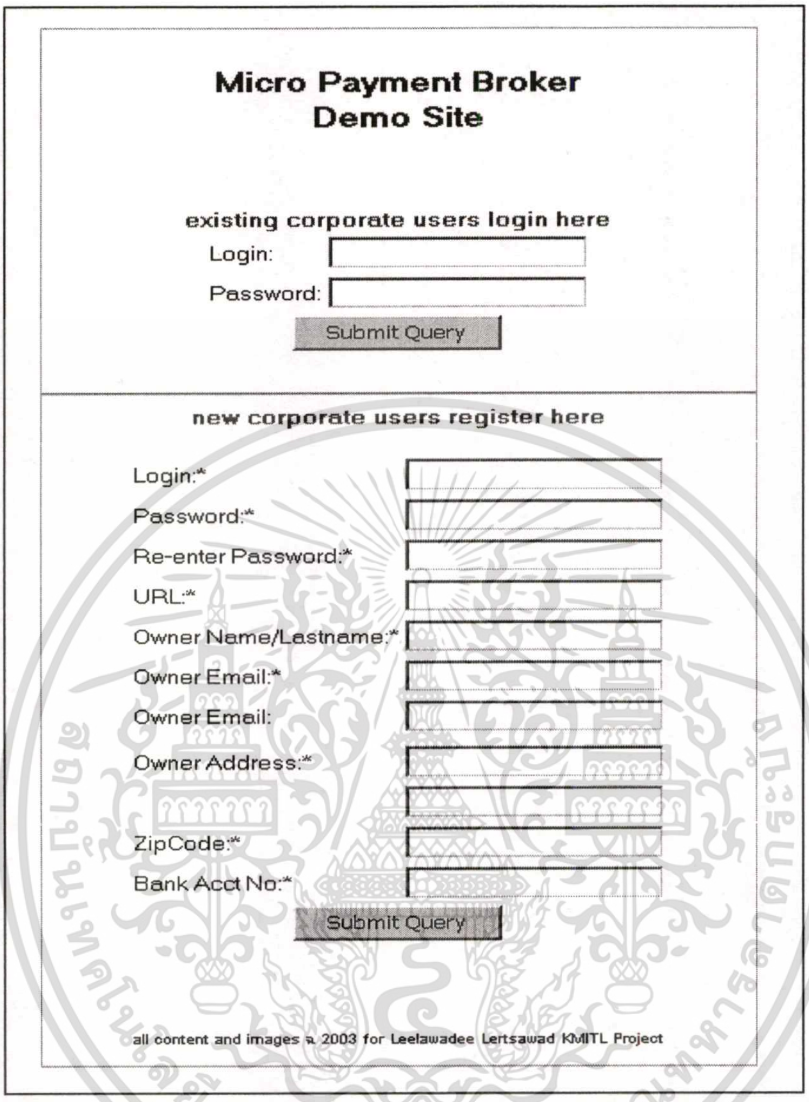


รูปที่ 3.14 แสดงหน้าจอการ เข้าไปดูประวัคิการเติมเงิน

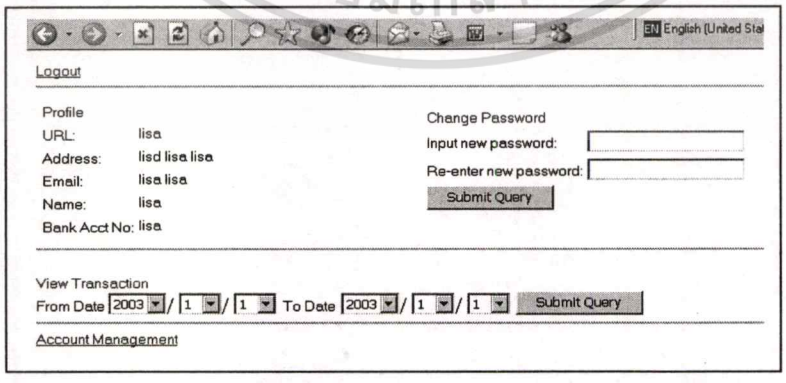
ในการดูประวัติ สามารถ click “Click to view Coupon History”
และสามารถดูรายการต่างๆของตนได้โดยใส่ date range ใน “View Transaction”



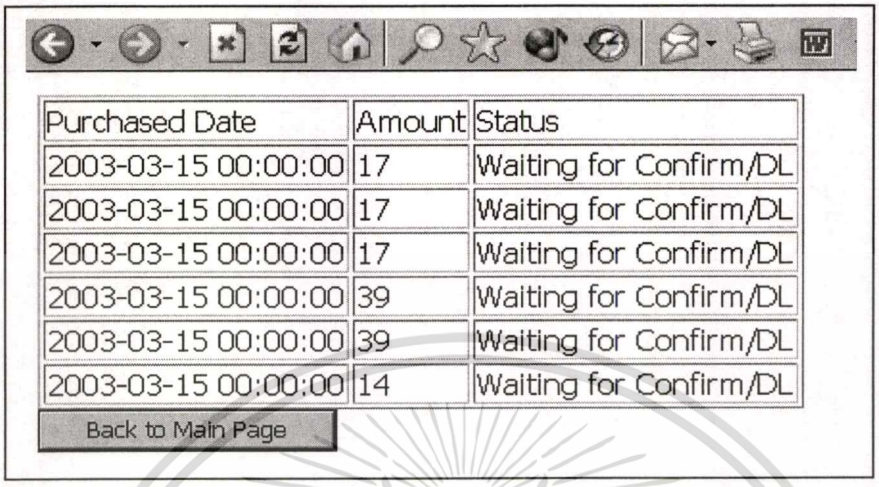
รูปที่ 3.15 แสดงหน้าจอรายการต่างๆของ User



รูปที่ 3.16 แสดงหน้าจอการ login ของ vendor และสมัครสมาชิกใหม่ของ vendor



รูปที่ 3.17 แสดงหน้าจอการ Manage System ของ vendor

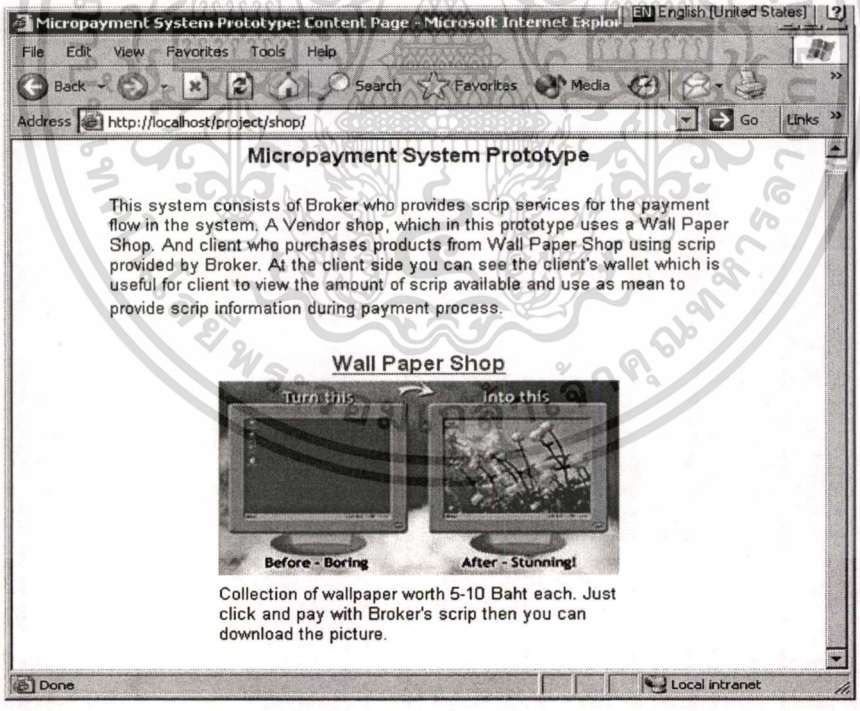


Purchased Date	Amount	Status
2003-03-15 00:00:00	17	Waiting for Confirm/DL
2003-03-15 00:00:00	17	Waiting for Confirm/DL
2003-03-15 00:00:00	17	Waiting for Confirm/DL
2003-03-15 00:00:00	39	Waiting for Confirm/DL
2003-03-15 00:00:00	39	Waiting for Confirm/DL
2003-03-15 00:00:00	14	Waiting for Confirm/DL

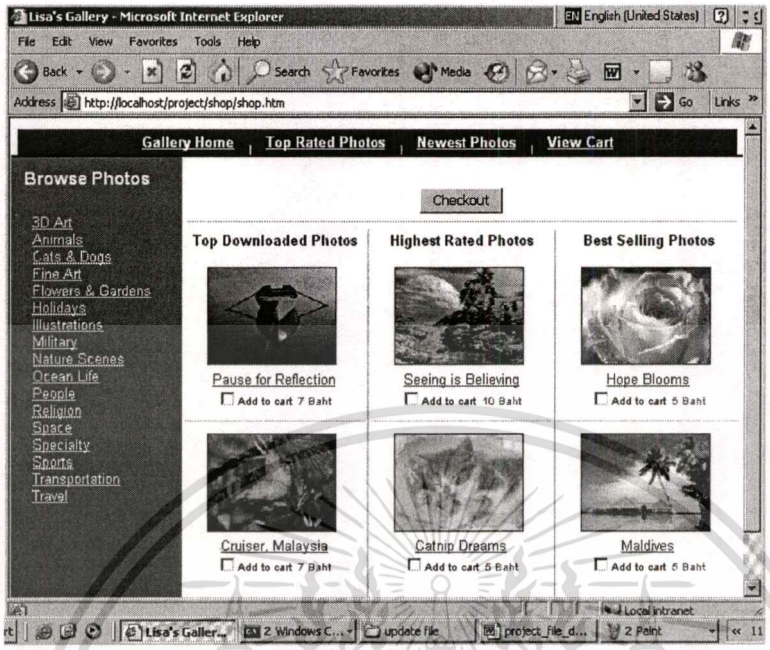
Back to Main Page

รูปที่ 3.17 แสดงหน้าจอการ View Transaction ของ vendor

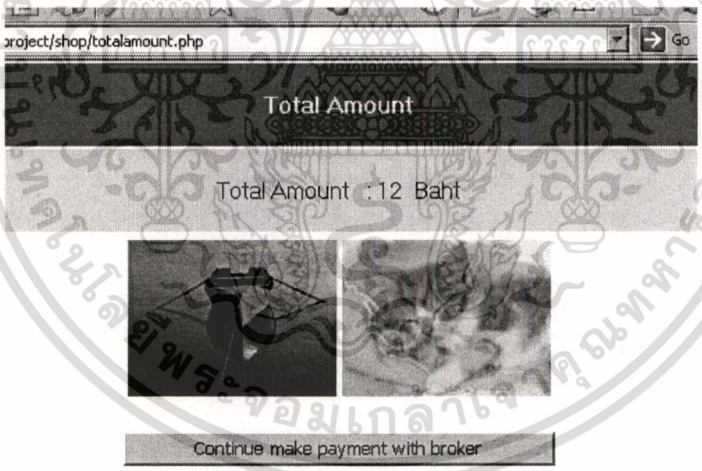
เริ่มต้นเข้าการทำรายการกับระบบ โดยเข้าร้านค้าจำลอง



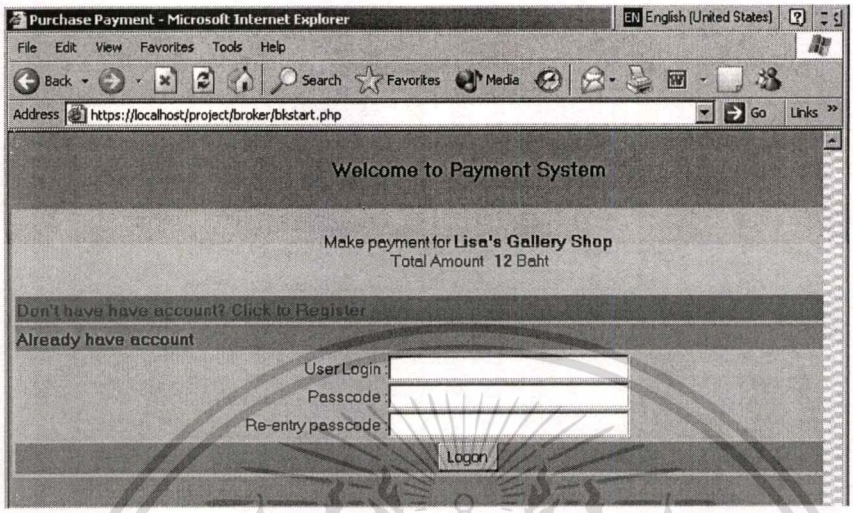
รูปที่ 3.18 แสดงหน้าจอร้านจำลอง



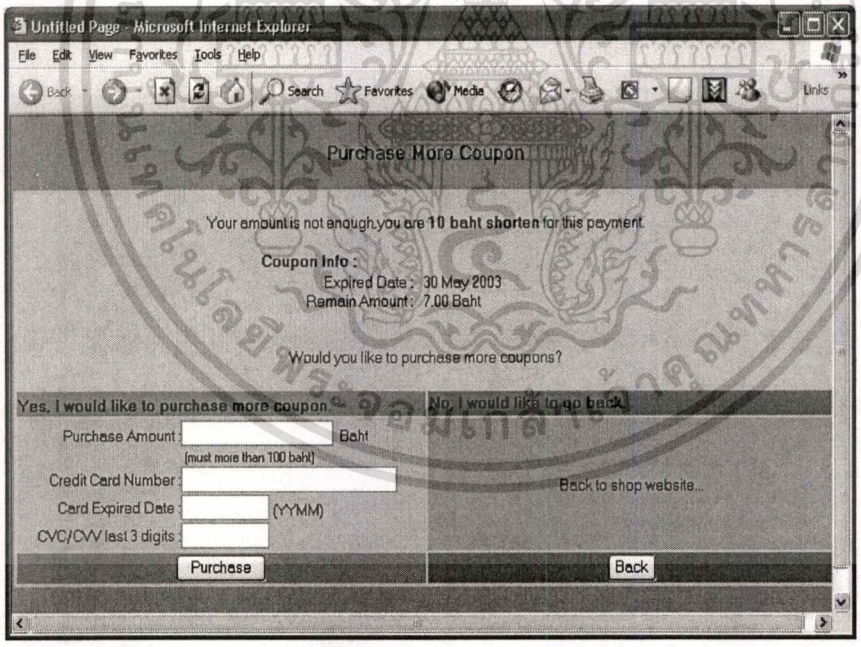
รูปที่ 3.19 แสดงหน้าจอขายของร้านจำลอง



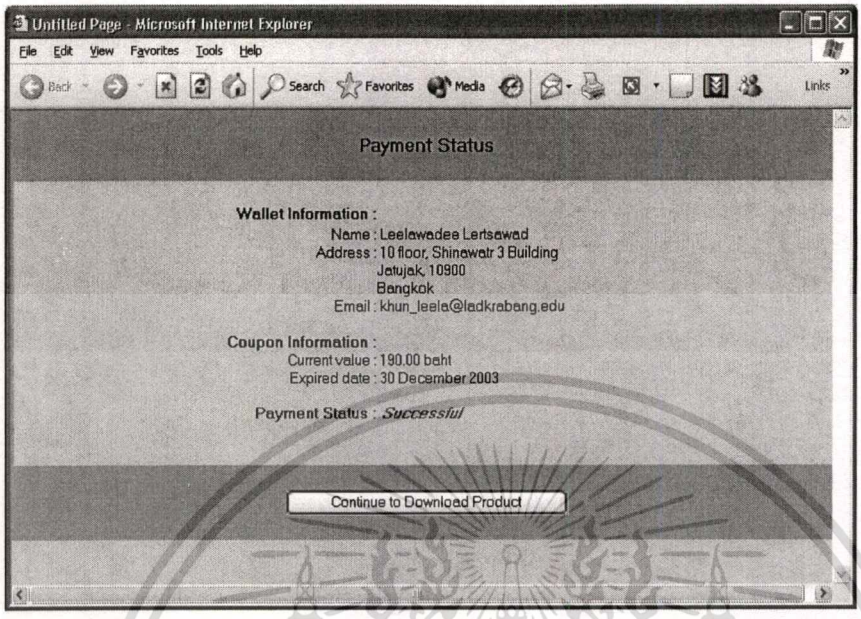
รูปที่ 3.20 แสดงหน้าจอการสรุปมูลค่าสินค้า



รูปที่ 3.21แสดงหน้าจอการกรอก Coupon Passcode



รูปที่ 3.22 แสดงหน้าจอซื้อ e money เพิ่มหากเงินไม่พอในขั้นตอนการซื้อ



รูปที่ 3.23 แสดงหน้าจอผลการชำระ e money

3.5 ความปลอดภัยของระบบ

- User มั่นใจในมูลค่าคงเหลือ

การทำรายการเข้ามาของลูกค้าเป็นเหมือนกับการขอ Authorize บัตรเครดิต คือ มูลค่า coupon จะยังไม่ถูกหักออกทันทีหากแต่จะหักก็ต่อเมื่อ Broker ได้สัญญาณจาก Vendor ก่อนเท่านั้น

- Secure Socket Layer

การทำธุรกรรมต่างๆกับ Broker จะผ่าน SSL ที่ผ่านการรับรองจาก Certificate Authority ที่น่าเชื่อถือ ในระบบจำลองที่ออกแบบมานี้ใช้ ของ thawte

- การเก็บข้อมูล

การเก็บข้อมูลที่สำคัญจะใช้ Hashing Algorithm เข้ามาช่วย เช่น login password, coupon passcode, vendor bank acct no, vendor user password

- การซื้อ coupon

ถูกออกแบบมาให้ใช้กับ Payment Gateway ที่มีความน่าเชื่อถือ

- การโอนเงินเข้าบัญชี

ถูกออกแบบมาให้ใช้กับ Payment Gateway ที่มีความน่าเชื่อถือ

บทที่ 4
การติดตั้งระบบ

4.1 องค์ประกอบของระบบที่พัฒนา

4.1.1 ฝั่ง Server ของผู้ให้บริการ

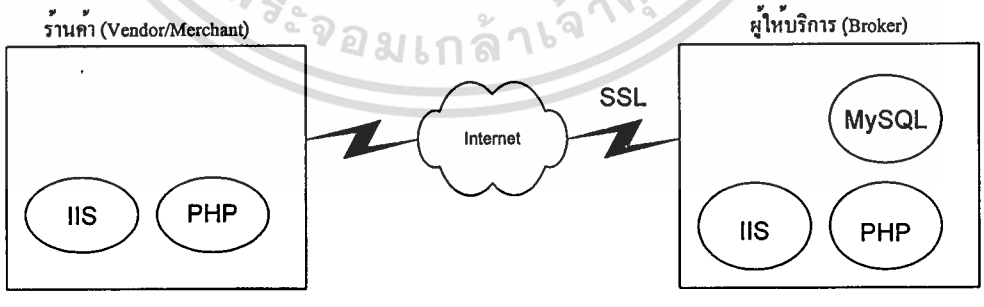
ระบบในฝั่ง server ของผู้ให้บริการจะประกอบไปด้วย

- Web Server IIS
- SSL
- PHP Server
- MySQL Server

4.1.2 ฝั่ง Server ของร้านค้า

ระบบในฝั่ง server ของผู้ให้บริการจะประกอบไปด้วย

- Web Server IIS
- PHP Server

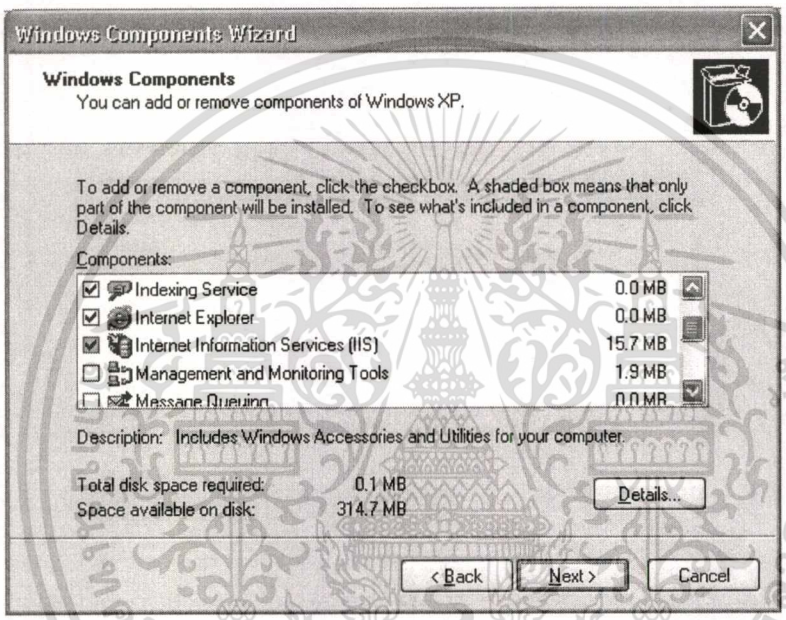


รูปที่ 4.1 แสดงสถาปัตยกรรมของระบบ

4.2 ขั้นตอนการติดตั้งบน Server

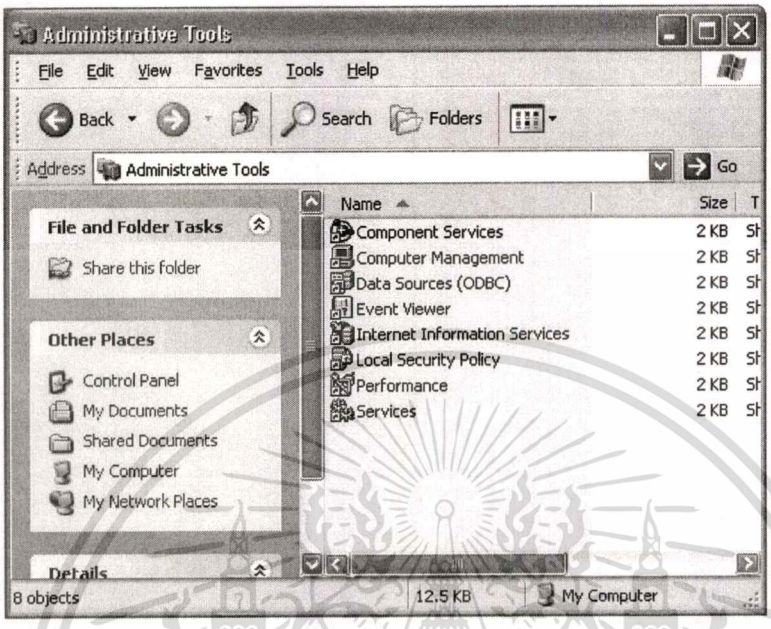
4.2.1 Web Server IIS Version 5.1

ใน Windows XP Professional ได้รวมเอา IIS เป็นคอมโพเนนต์หนึ่งใน Windows และกลายเป็นเซอร์วิสที่ชื่อว่า Internet Information Services สำหรับการติดตั้งสามารถเข้าไปที่ Control Panel -> Administrative Tools -> Add/Remove Program -> Add/Remove Windows Components จากนั้นเลือก Internet Information Services (IIS)



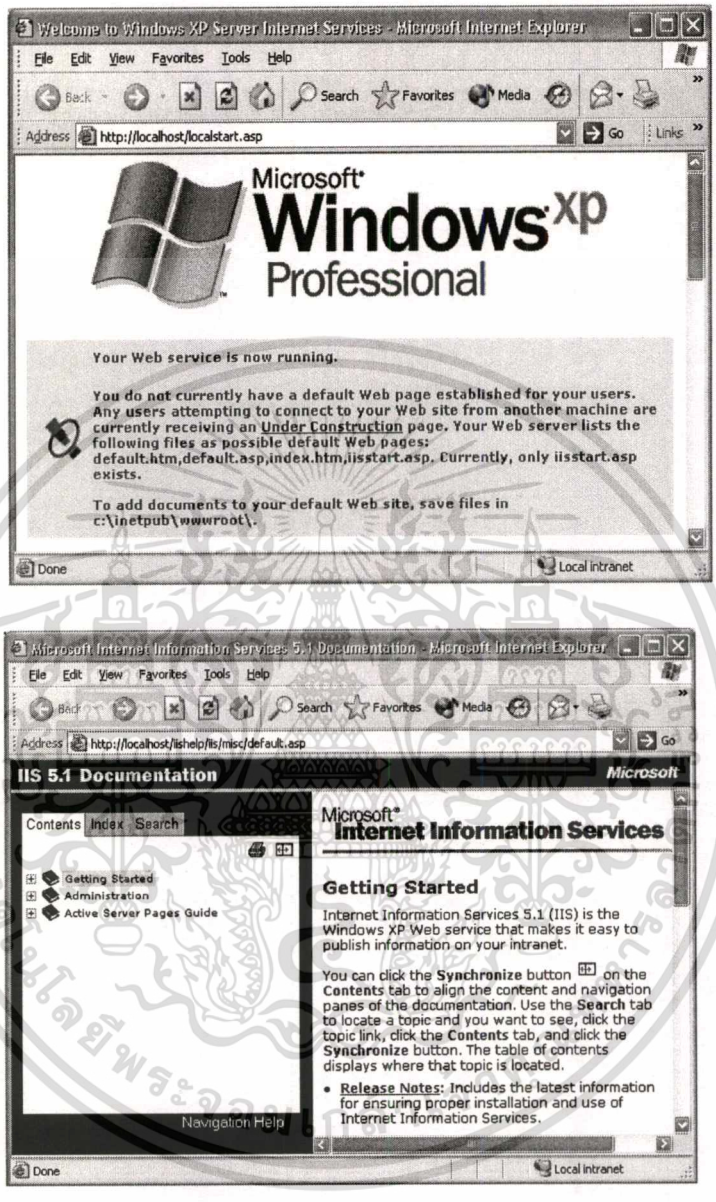
รูปที่ 4.2 แสดงการติดตั้ง IIS

เมื่อลงเสร็จจะปรากฏ IIS icon ขึ้นใน Admistrative Tool ดังรูป



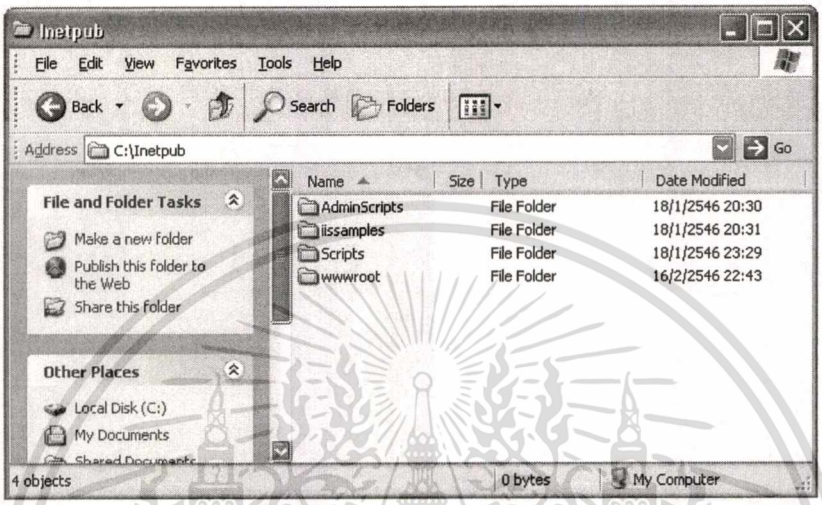
รูปที่ 4.3 แสดงการติดตั้ง IIS (ต่อ)

เมื่อติดตั้งเสร็จสามารถทดสอบการทำงานของ IIS ได้โดยเปิดบราวเซอร์โดยใส่ URL เป็น http://localhost/ จะได้เว็บเพจดีฟอลต์แสดงคำอธิบายการติดตั้งเว็บเพจบน Windows XP Professional และคุณสมบัติและคูมือ IIS 5.1 พร้อมเอกสารคำแนะนำดังรูปตามลำดับ



รูปที่ 4.4 แสดงการผลทดสอบหลังติดตั้ง IIS

หลังจากที่ได้ทำการติดตั้ง IIS เรียบร้อยแล้ว ระบบจะทำการสร้างโฟลเดอร์ Inetpub ไว้ที่รากไดเร็คทอรี (Root Directory) ซึ่งภายในจะประกอบด้วยไดเร็คทอรีย่อยๆ เกี่ยวข้องกับการทำงานของระบบดังนี้



รูปที่ 4.5 แสดงการผลของระบบหลังติดตั้ง IIS

ตารางที่ 4.1 ไดเร็คทอรีและคำอธิบายหลังติดตั้ง IIS

ไดเร็คทอรี	คำอธิบาย
AdminScripts	เก็บไฟล์ของ IIS Adminitration สคริปต์ สำหรับ Windows Scripting Host
iisamples	เก็บตัวอย่างเกี่ยวกับ IIS
Scripts	เป็นดีฟอลต์สำหรับเก็บสคริปต์ หรือแอพพลิเคชั่นซึ่งถูกใช้โดยดีฟอลต์เว็บไซต์รวมถึงตัวอย่าง และเครื่องมือต่างๆ
wwwroot	เป็นรากไดเร็คทอรีสำหรับดีฟอลต์เว็บไซต์ (WWW)

4.2.2 การติดตั้ง SSL บน IIS

การติดตั้ง SSL สามารถทำได้โดยสร้างตัวขอ request certificate ได้จาก

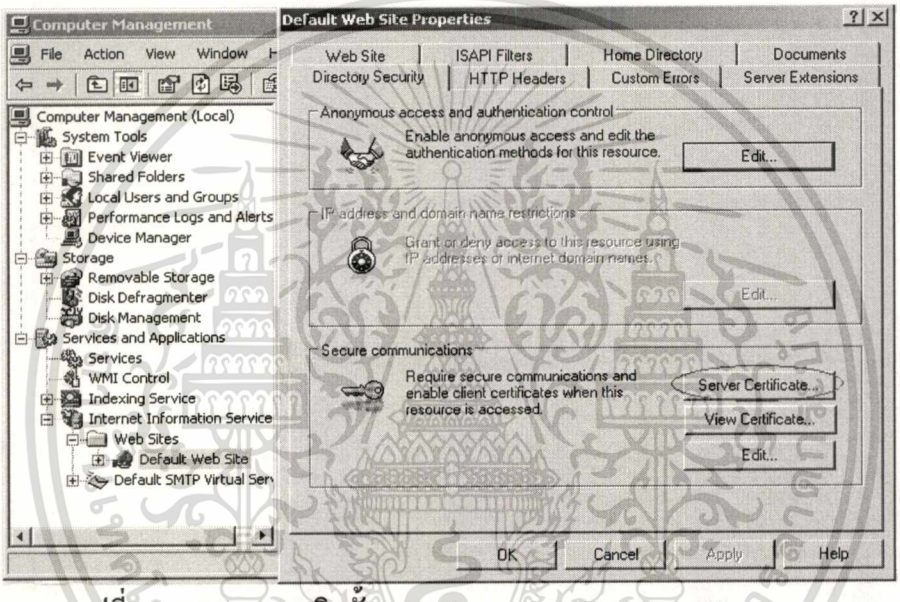
Computer Management -> Services and Application

-> Internet Information Services -> Web Sites -> Default Web Sites

และ mouse right click -> Properties -> Directory Securities

-> Server Certificates -> Create New Certificates จากนั้นจะได้ file certreq.txt

ซึ่งเป็น Key ที่ใช้ในการร้องขอ SSL Certificate จาก Certificate Authority



รูปที่ 4.6 แสดงจุดการติดตั้ง Web Server Certificate for IIS

หน้าตาของ certreq.txt

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDTTCCArYCAQAwcjESMBAGA1UEAxMJYmtrbHN4cDFhMRswGQYDVQQLExJQcm9q
ZWN0IE1hbmFnZW1lbnQxFjAUBgNVBAoTDUxlZWxhIFByb2plY3QxDDAKBgNVBAcT
A0JLSzEMMAoGA1UECBMDQktLMQswCQYDVQQGEwJVUzCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEAr0D15NfX5pXoF9fTVNEfwmAU/o8gnNYKxSPgDTRAc4qLHXZZ
K+qtDeSywi3iuJf9I1dAz/a8PjPElZubdFwRNZmUDfsqcFrObUE6rjNZXLG1ileX
gmDP3jpL6+ZjlgMV8gSmJyI6tWSN7s+L4kZJ40RGvbgYX5J9dBAFyvxvSjsCAwEA
AaCCAZkwGgYKKwYBBAGCNw0CAzEMFgo1LjEuMjYwMC4yMHsGCisGAQQBgjcCAQ4x
bTBrMA4GA1UdDwEB/wQEAwIE8DBEBgkqhkiG9w0BCQ8ENzA1MA4GCCqGSIb3DQMC
AgIAgDAOBggqhkiG9w0DBAICAIAwBwYFKw4DAgcwCgYIKoZIhvcNAwcwEwYDVR0l
BAwwCgYIKwYBBQUHAwEwgf0GCisGAQQBgjcNAgIxge4wgesCAQEeWgBNAGkAYwBy
AG8AcwBvAGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuAG4AZQBsACAAQwByAHkAcAB0
AG8AZwByAGEAcABoAGkAYwAgAFAAcgBvAHYAaQBkAGUAcgOBiQCqEH3QppP7Ewuz
6oh4EUXMbKdqieAcbQ52iFSXqQ/n1xAtEpVUfjIM3exr42EhyYlrlV7cpUKbSr/e
Q6c/hjiUi17EpvleBBV0BkFWsWzJoShx0BmOKvDnKINNQC3Jya+MN/t9axyuCwdU
YJiLglNnjcBLSxL/6hovXNDLuCLgMAAAAAAAAAAAMA0GCSqGSIb3DQEBBQUAA4GB
ADQEd9THPV1cybryc1bPvKMvrRwQRnSD+tC42iiVKel8SdoLDcNjeTJLS9NBLUgs
rcwTAAFjjed5seSENRb5uVPaqt6C70hXzgNKzlZMRG7Yq1XcQaJcx6fFLSpYXNrs
5pyp4bKUL/n/rS5AkZX8dR9Olj3sDz+rO8e0cEHFTUI+
-----END NEW CERTIFICATE REQUEST-----
```

ขั้นตอนต่อไป ต้องส่งการร้องขอดังกล่าวไปให้ Certificate Authority ในที่นี้ใช้ Thawte เข้า http://www.thawte.com -> Products -> Web Server Certificates -> try -> Register

จากนั้นเข้าสู่ขั้นตอนการสร้าง Certificate

■Step 1 - Choosing a test certificate

Here's where you choose the type of test certificate you want to generate, such as a test Web Server Certificate or a generic mix-and-match Custom Certificate. Tick which one suits you best.

◉ Test X509v3 SSL Cert (preferred)

○ Test X509v1 SSL Cert

NOTE: Thawte only issues x509v3 certificates!

■Step 2 - Choosing the format for your test certificate

We can deliver certificates in a number of different formats - here's where you select what will work best with your server.

Go for the default format if you are getting a standard test certificate, such as a Web Server SSL test Certificate

◉ **Use the default for your kind of certificate**
This will auto-select the format to be used based on the kind of test certificate and the format of your CSR.sslv3

○ **Use the "standard" format**
This is the lowest-common-denominator format is a BASE64 encoding of an X509 certificate.

○ **Use PEM Format**
This isn't our favourate format, but you probably need this if your CSR has these words in it:
-----BEGIN PRIVACY-ENHANCED MESSAGE-----
Please note that we can only generate this format if your CSR is itself a PEMmessage. (You can still choose to have X509v3 certificate, and have some of the above extentions embedded.)

■Step 3 - Certificate Signing Request

Please copy and paste your Certificate Signing Request into the space below.
Here's what it **should** look like:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBPTCB6AIBADCBhDELMAkGA1UEBhMCWkExFTATBgNVBAgTDFdlc3Rlcm4gQ2Fw
ZTESMBAGA1UEBxMJQ2FwZSBUb3duMRQwEgYDVQQKEwtPcHBvcnR1bml0aTEYMBYG
A1UECxMPT25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3cuZm9yd2FyZC5jby56
YTBaMA0GCSqGSIb3DQEBAQUAA0kAMEYCQQDT5oxxeBWu5WLHD/G4BJ+PobiC9d7S
6pDvAjuyC+dPAnL0d91tXdm2j190D1kgDoSp5ZyGSgwJh2V7diuuPlHDAgEDoAAw
DQYJKoZIhvcNAQEEBQADQQBf8ZHIu4H8ik2vZQngXh8v+iGnAXD1AvUjuDPCWzFu
pReiq7UR8Z0wiJBeaqiuvTDnTFMz6oCq6htdH7/tvKhh
-----END CERTIFICATE REQUEST-----
```

Please don't forget:

- If you don't know what a **CSR** is, please review your web server documentation on the generation of server certificate requests, or ask your server administrator.
- **IIS5 / Win2K users:** After trying a test certificate, please don't request a trusted certificate using the same Certificate Signing Request (CSR). Replacing a test certificate becomes ***enormously complicated*** if you've used the same key and CSR!

■ **Here is your certificate:**

```
-----BEGIN CERTIFICATE-----
MIIClzCCAgCgAwIBAgIDan8PMA0GCSqGSIb3DQEBBAUAMIGHMQswCQYDVQQGEwJa
QTEiMCAGA1UECBMZRk9SIFRFU1RJTkcgUFVSUE9TRVMgT05MWTEdMBsGA1UEChMU
VGhhd3RlIENlcnRpZmljYXRpb24xFzAVBgNVBAsTDlRFU1QgVEVTVCBURVNUMRww
GgYDVQQDExNUaGF3dGUgVGVzdCBDQSBSb290MB4XDTAzMDMwODA5NDkwMFoXDTAz
MDMyOTA5NDkwMFowcjESMBAGA1UEAxMJYmtrbHN4cDFhMRswGQYDVQQLExJQcm9q
ZWN0IE1hbmFnZW1lbnQxFjAUBgNVBAoTDUxlZWxhIFByb2plY3QxDDAKBgNVBAcT
A0JLSzEMMAoGA1UECBMDQktLMQswCQYDVQQGEwJVUzCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEAr0D15NfX5pXoF9fTVNEfwmAU/o8gnNYKxSPgDTRAc4qLHXZZ
K+qtDeSywi3iuJf9I1dAz/a8PjPElZubdFwRNZmUDfsqcFrObUE6rjNZXLG1ileX
gmDP3jpL6+ZjlgMV8gSmJyI6tWSN7s+L4kZJ40RGvbgYX5J9dBAFyvxvSjsCAwEA
AaMlMCMwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDAYDVR0TAQH/BAIwADANBgkqhkiG
9w0BAQQFAAOBgQCjF+U3NSewYZoKwsE3/SiieCY9i42GkusOa6RU9edtCQ2nxYDc
WlJG47VbQoaZdd5SrM9vUkXGBbAE7mOkxkChpkdSnFeNlJj778lGHoICnplT1/h2
rQMeQFEKp427Qb3GqJYJkq4pOs4r0ZgE+oxkqu5TV9Nlv7AlHYCtBGXDsg==
-----END CERTIFICATE-----
```

Note: The certificate displayed above needs to be copied and pasted into a file on the machine where you will be utilising it; it is not installed automatically on your web server. Please make sure that you attach it to the private key from which it was originally created.

Test certificates created by this system are untrusted by browsers/web servers. To ensure that you create a seamless Test environment it is recommended you download the Test Root certificate into your browser, which will ensure that your Test certificate is trusted. Download the Root certificate here:

http://www.thawte.com/html/SUPPORT/keygen/servertest.crt

นำ Certificate ที่ได้ไป copy ใส่ไฟล์บนเครื่องเว็บเซอร์เวอร์ แล้วจากนั้นเข้าไปติดตั้งบน IIS ที่

Computer Management -> Services and Application

-> Internet Information Services -> Web Sites -> Default Web Sites

และ mouse right click -> Properties -> Directory Securities

-> Server Certificates -> Proceed pending request -> browse to new received (copied) Certificate file -> SSL ready!

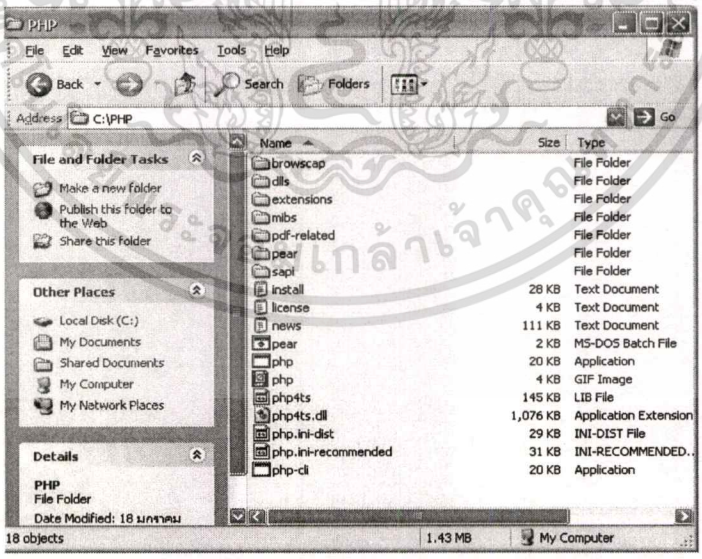
จากนั้นสามารถเข้าไปเรียกใช้เว็บเซอร์เวอร์แบบผ่าน Protocol SSL ได้ เช่น

https://localhost/project/broker/index.htm

4.2.3 PHP Server 4.2.3 for Windows

ดาวน์โหลดไฟล์ PHP version 4.2.3 (php-4.2.3-Win32.zip) จากเว็บไซต์ www.php.net จากนั้นนำมา unzip ใส่เครื่อง จากนั้นเริ่มทำการติดตั้งโดยทำตามขั้นตอนจากไฟล์ install.txt ที่ติดมากับไฟล์ที่ได้ดาวน์โหลดมา

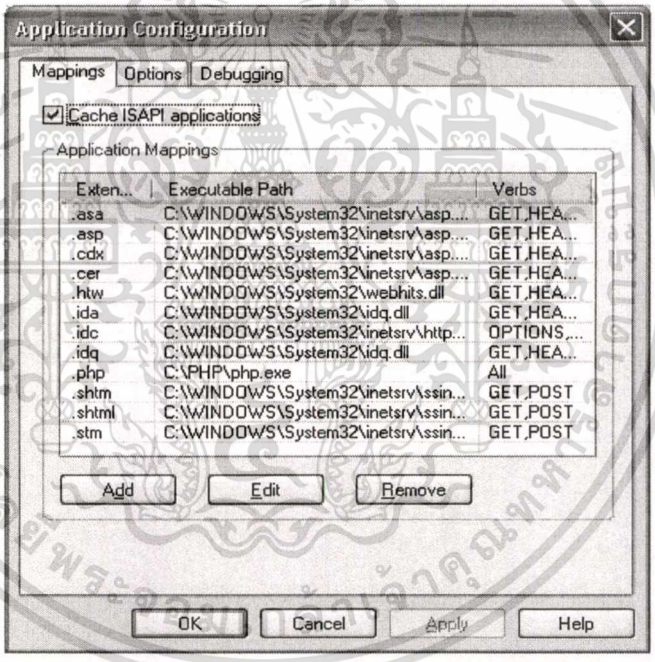
จากนั้นจะได้ directory C:\PHP ที่มีข้อมูลดังรูป



รูปที่ 4.7 แสดงการติดตั้ง PHP Server for Windows

โดยในขั้นตอนที่ผู้เขียนเลือกทำคือเลือกที่จะติดตั้งเป็นแบบ CGI บน IIS version 5.1 ดังนั้นสิ่งที่ต้องทำคือ

- copy php.ini และ browscap.ini ไปใส่ที่ directory C:\windows
- จากนั้นแก้ไขการตั้งค่าบางตัวในไฟล์ php.ini ให้เป็นไปอย่างที่เหมาะสมกับการใช้งาน
- เข้าไป add ใน IIS ให้รู้จัก extension .php ที่ Control Panel -> Administrative Tools -> Internet Information Services คลิกเข้าไปจะปรากฏหน้าต่าง Internet Information Services ให้เลือกไปที่ Default Web Site และเลือก Properties จะได้หน้าต่าง Default Web Site Properties ขึ้นมา
  ให้เลือกไปที่ Home Directory และคลิก Configuration จะปรากฏหน้าต่าง

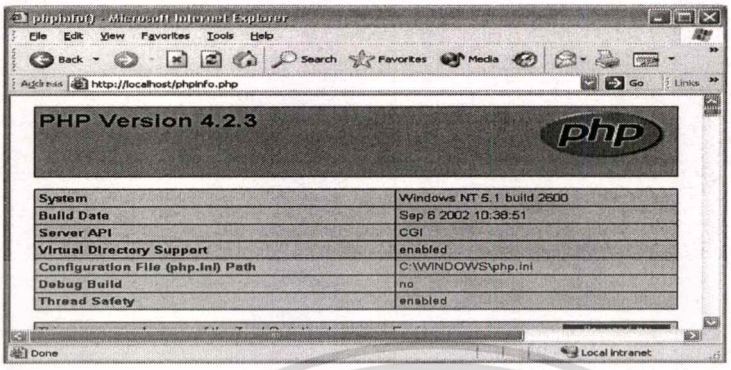


รูปที่ 4.8 แสดงการเพิ่ม Extension file .php ในระบบของ Web Server

Application Configuration ให้เพิ่ม Application Mappings ตัวใหม่เข้าไปโดยคลิกปุ่ม Add โดยใส่ Extension เป็น .php และใส่ Executable Path เป็น C:\PHP\php.exe

จากนั้นสามารถทดสอบการทำงานของ PHP ได้โดยเขียนสคริปสั้นๆ และเปิดจากบราวเซอร์ <?php phpinfo(); ?> จะได้ข้อมูลรายละเอียดของ parameter

ต่างๆ ณ ปัจจุบันของเว็บเพจนั้นๆ



รูปที่ 4.9 แสดงผลการทดสอบหลังการติดตั้ง PHP Server

จากนั้นสามารถเริ่มพัฒนาโปรแกรมด้วยภาษา PHP ได้บน windows platform

4.2.3 MySQL Server

เข้าไปดาวน์โหลดไฟล์ MySQL version 3.23.54 (mysql-3.23.54-win.zip) ได้จาก www.mysql.com จากนั้นนำมาติดตั้งโดย upzip ไฟล์และ run setup.exe ที่ให้มากับไฟล์ เมื่อ install เรียบร้อยสามารถเรียกใช้งาน mysql ได้โดย

- สั่งให้ mysql เริ่มทำงานเป็นเซอร์วิสใน windows จากคำสั่ง mysqld-nt –install
- เข้าไป start การทำงานของ mysql จากคำสั่ง mysqld-nt –standalone

จากนั้นจึงเริ่ม create database และ create table ต่างๆในระบบ

บทที่ 5
สรุปและข้อเสนอแนะ

5.1 บทสรุป

อัตราการเติบโตของอินเตอร์เน็ตมีการเติบโตสูงในแง่ของการค้นหาสืบค้นหาข้อมูลประเภทดิจิตอลเป็นอย่างมาก เช่น ซอฟต์แวร์ ข้อมูลข่าว ข้อมูลดัชนีหุ้น เพลง รูปภาพ วีดีโอไฟล์ และ ข้อมูลค้นคว้ารายงาน ทั้งนี้ในแง่ของผู้ให้บริการ การที่จะเรียกเก็บค่าบริการเป็นเรื่องที่มีเหตุผล เพราะการจะได้มาซึ่งข้อมูลนั้นต้องใช้ทรัพยากรมากมาย แต่ในแง่ของผู้บริโภคยังไม่คุ้มที่จะเสียค่าใช้จ่ายในการชำระมูลค่ามากๆ เพื่อสมัครสมาชิก เพียงเพื่อใช้งานเอกสารชิ้นเดียว

ดังนั้น ไมโครเพย์เมนต์ ดูจะเป็นทางออกสำหรับผลิตภัณฑ์ประเภทนี้ เพราะผู้บริโภคสามารถเลือกจ่ายได้ทีละน้อย ข้อได้เปรียบต่อผู้บริโภคเมื่อมี ไมโครเพย์เมนต์ คือผู้บริโภคไม่จำเป็นต้องซื้อเป็นแพ็คแต่สามารถซื้อแยกย่อยเฉพาะหน่วยที่ต้องการได้

สรุปประโยชน์หลักของระบบ

- สามารถนำทฤษฎีของ ไมโครเพย์เมนต์ ที่มีในปัจจุบัน มาพัฒนาและประยุกต์ให้เข้ากับพาณิชย์อิเลคโทรนิกส์ของเว็บไซต์ไทยได้
- ส่งเสริมให้เกิดการแข่งขันด้านผลิตภัณฑ์ข้อมูลออนไลน์ให้มีประสิทธิภาพยิ่งขึ้น
- ผู้บริโภคมีโอกาสในการเลือกผลิตภัณฑ์มากขึ้น และอำนวยความสะดวกให้ผู้บริโภคได้มีช่องทางการชำระเงินที่หลากหลายขึ้น
- เป็นต้นแบบให้กับการพัฒนาการชำระเงินแบบ ไมโครเพย์เมนต์ ในระบบพาณิชย์อิเลคโทรนิกส์ของเว็บไซต์ไทย

สรุปประโยชน์เสริมของระบบ

- ผู้ทำได้เกิดความเข้าใจในระบบไมโครเพย์เมนต์ ทั้งที่มีในปัจจุบันและที่ได้นำมาปรับเปลี่ยนให้เข้ากับการใช้งานในร้านค้าของไทยในปัจจุบัน
- ได้เข้าใจวิธีการสร้างระบบที่มี Secure Socket Layer (SSL)

5.2 ข้อเสนอแนะ

จุดสำคัญที่ต้องคำนึงถึงคือระบบความปลอดภัยที่น่าเชื่อถือ
ทั้งในแง่

- ความปลอดภัยในการเก็บข้อมูลในระบบไม่ให้ถูกอ่านได้
- ความปลอดภัยในการรับส่งข้อมูลระหว่างคู่ค้า
- ควรหาวิธีแลกเปลี่ยนข้อมูลที่มีความปลอดภัยและลงทุนต่ำ และมีประสิทธิภาพที่ทำให้การแลกเปลี่ยนข้อมูลสามารถทำได้ในเวลารวดเร็ว

การออกแบบและพัฒนาระบบการชำระเงินในระบบนี้ได้เน้นให้เห็นถึงการให้บริการของ Broker เป็นหลัก เพราะจัดว่าเป็นหัวใจของระบบ ดังนั้นจึงต้องคำนึงถึงส่วนนี้เป็นหลัก

บรรณานุกรม

Amir Herzberg. 1998. **Safeguarding Digital Library Contents.** D-Lib Magazine [Online] Available: http://www.dlib.org/dlib/january98/ibm/01herzberg.html.

Chi, Ellis. 1997. **Evaluation of Micropayment Schemes.** [Online] HP Labs Technical Reports Available: http://www.hpl.hp.com/techreports/97/HPL-97-14.html.

MySQL. 2003. **MySQL 3.23 Declared Stable** [Online] Available: http://www.mysql.com/news/article-54.html.

Port Paye. 2003. **The Micropayment Solution** [Online] Available: http://www.portpaye.com.

Ronald Rivest et.al. 1996. **PayWord and MicroMint: Two simple micropayment schemes.** Security Protocols Workshop.

S. Glassman et.al. 1995. **The MilliCent Protocol for Inexpensive Electronic Commerce.** Fourth International World Wide Web Conference.

Thawte. 2003. **Web Server Certificates** [Online] Available: http://www.thawte.com/html/RETAIL/ssl/index.html.

The PHP Group. 2001-2003. **Download documentation.** [Online] Available: http://www.php.net/download-docs.php.

Thierry Michel. 2001. **Micropayments Overview.** [Online] W3C Technology and Society domain. Available: http://www.w3.org/ECommerce/Micropayments/Overview.html.

Transaction Net. 2003. **Micropayment Methods.** [Online] Available: http://www.transaction.net/payment/micro.html.

Verisign Inc. **Get the Plans to Build a Secure E-Commerce Infrastructure.** [Online] Available: http://www.verisign.com/cgi-bin/clearsales_cgi/leadgen.htm.

Xiaoling Dai et.al. **Comparing and contrasting micro-payment models for E-commerce systems.** Department of Computer Science, University of Auckland.

ประวัติผู้เขียน

ชื่อ	นางสาวลีลาวดี เลิศสวัสดิ์
การศึกษา	ปริญญาตรีมหาวิทยาลัยอัสสัมชัญ คณะวิศวกรรมศาสตร์ ภาคคอมพิวเตอร์
การทำงาน	บริษัทอมาเดอุสเอเชีย แผนก e-Commerce
วันเดือนปีเกิด	20 มิถุนายน 2518
สถานที่เกิด	กรุงเทพมหานคร