ซ้อนของการทำงาน ไม่ต้องมานั่งป้อนข้อมูลซ้ำ มานั่งเดาเอกสารที่ไม่ชัด หรือว่าจะมีกระบวนการอื่นๆอีกไหมที่จะเพิ่มประสิทธิภาพในการทำการค้า ให้พิจารณาดูเรื่องคู่ค้าของบริษัทว่าต้องติดต่อกับใคร อาจเป็นผู้บริโภคทั่วไป ซัพพลายเออร์ เป็นภาครัฐ หรือว่าตัวเราเองเป็นซัพพลายเออร์ให้กับคู่ค้า เมื่อทราบชัดเจนแล้วเริ่มหาข้อมูลว่าในธุรกิจรูปแบบที่ดำเนินอยู่นี้เขาใช้พาณิชย์อิเล็กทรอนิกส์กันหรือไม่อย่างไร และพิจารณาดูว่าคุณมีความพร้อมจะทำอย่างนั้นหรือยัง และจำเป็นหรือไม่อย่างไร

ระดับการใช้งาน

ตามที่ได้กล่าวไว้แล้วว่าก่อนที่จะลงทุนในการพัฒนาควรจะมีการศึกษาก่อนว่าความจำเป็น ความต้องการใช้งานอยู่ในระดับใด อาจจะแบ่งได้ 3 ระดับคือ

ระดับที่หนึ่ง ใช้อินเทอร์เน็ตและบริการที่มีให้ใช้มาวางแผนเพื่อช่วยในการทำการค้า ในระดับนี้คือการพิจารณานำเอาสิ่งที่มีให้ใช้เป็นพื้นฐานอยู่แล้วในอินเทอร์เน็ต เช่น อาจจะใช้อีเมล์ในการติดต่อลูกค้า สอบถามข้อมูล ตอบข้อมูลให้ลูกค้า โฆษณาสินค้าใหม่ๆ หรือจะใช้ในการหาข้อมูลคู่แข่งขัน สภาพตลาด ดูสินค้าคู่แข่งใหม่ๆ ซึ่งสิ่งนี้สามารถเริ่มได้ไม่ยากและใช้งานได้ง่ายมากในปัจจุบัน ค่าใช้จ่ายก็ไม่แพงแล้ว สามารถหาซื้อ Starter Kit ได้ตามร้านสะดวกซื้อทั่วไป แต่ก่อนอื่นท่านก็ต้องมีเครื่องคอมพิวเตอร์พร้อมโมเด็มและสายโทรศัพท์รอไว้ก่อน

ระดับที่สอง สร้างเว็บไซต์เพื่อทำการให้ข้อมูล/ประชาสัมพันธ์ ลงทุนไม่มากนักกับการสร้างเว็บไซต์สำหรับบริษัท ในการให้ข้อมูลของบริษัทเอง สถานที่ตั้ง เบอร์โทรศัพท์ โทรสาร หรือช่องทางการติดต่ออื่นๆ การให้ข้อมูลสินค้า การใช้งานสินค้า การให้บริการหลังการขาย สร้างฐานข้อมูลคำถามที่ถามบ่อย (Frequently Asked Questions – FAQs) เพื่อให้ลูกค้าสามารถแก้ปัญหาเองได้ขั้นต้น และควรสร้างช่องทางการให้ความคิดเห็นจากลูกค้าอย่างสะดวกด้วย

ระดับที่สาม พัฒนาให้ครบวงจร การจะให้เกิดการค้าที่ครบวงจรได้นั้นในทางพาณิชย์อิเล็กทรอนิกส์คือการสร้างให้สามารถทำการซื้อขายผ่านทางเว็บไซต์ได้ ในที่นี้ก็คือการสร้างระบบตะกร้าสินค้าและเชื่อมต่อกับระบบการชำระเงิน ซึ่งก็มีหลากหลายให้เลือกใช้ตามที่ได้กล่าวไว้ข้างต้น

นอกจากให้สามารถเกิดการซื้อขายได้แล้วนั้น ในการค้าบางรูปแบบอาจจะมีไปมากกว่านั้น คือการเชื่อมต่อระบบสำนักงานส่วนหลังบางส่วนเข้ากับอินเทอร์เน็ตให้คู่ค้าที่มีสิทธิทำการติดต่อโดยตรง เช่นการให้เข้ามาสำรวจสินค้าในสต๊อกว่ามีเพียงพอให้ทำการสั่งซื้อหรือไม่ หรือเชื่อมโยงกับคู่ค้าในเรื่องการจัดการห่วงโซ่การผลิต (Supply Chain Management)

สรุประดับการใช้งานเรียงจากระดับเบื้องต้นไปจนถึงซับซ้อนมาก

งาน จัดซื้อเครื่องคอมพิวเตอร์

ประโยชน์ที่ได้รับ ใช้งานโปรแกรมพื้นฐานทั่วไป เช่นพิมพ์จดหมาย ทำบัญชี บันทึกข้อมูลต่างๆในการทำการค้า

สิ่งที่ต้องจัดเตรียมเบื้องต้น --------

งาน ใช้อีเมล์ติดต่องาน แทนการใช้โทรศัพท์ โทรสาร จัดพิมพ์เอกสารประชาสัมพันธ์

ประโยชน์ที่ได้รับ รวดเร็วและมีประสิทธิภาพมากกว่าแบบเดิม ข้อมูลที่ส่ง เผยแพร่ สามารถสร้างให้มีลูกเล่น ทั้งภาพเคลื่อนไหว เสียง สามารถแจกเอกสาร

หรือทำการเผยแพร่ได้ในราคาถูก และถึงผู้รับในจำนวนมาก รวดเร็วในการได้รับคำแนะนำหรือการตอบรับจากลูกค้า
สิ่งที่ต้องจัดเตรียมเบื้องต้น คอมพิวเตอร์และโมเด็ม พร้อมทั้งสมัครเป็นสมาชิกใช้งานอินเทอร์เน็ตหรือซื้อชุดคิตมาใช้
งาน World Wide Web
ประโยชน์ที่ได้รับ
- หาข้อมูลประกอบการทำธุรกิจ
- ศึกษาตลาด ศึกษาคู่แข่ง
- เพิ่มช่องทางการจัดหา จัดซื้อสินค้า วัตถุดิบ
สิ่งที่ต้องจัดเตรียมเบื้องต้น คอมพิวเตอร์และโมเด็ม พร้อมทั้งสมัครเป็นสมาชิกใช้งานอินเทอร์เน็ตหรือซื้อชุดคิตมาใช้
งาน สร้างระบบรับสมาชิกทางอีเมล์และตอบอีเมล์อัตโนมัติ หรือระบบแฟกซ์อัตโนมัติ (Fax On demand System)
ประโยชน์ที่ได้รับ
- ส่งจดหมายข่าวหรือประกาศ โฆษณา ให้สมาชิก ที่ลงชื่อไว้
- ส่งคำสั่งซื้อสินค้าไปยังซัพพลายเออร์อัตโนมัติตามที่กำหนดไว้
- ส่งใบเตือนการชำระเงินไปยังคู่ค้า โดยอัตโนมัติ
สิ่งที่ต้องจัดเตรียมเบื้องต้น จัดหาซอฟต์แวร์สำเร็จรูปมาใช้
- จัดจ้าง/พัฒนาบุคลากร เพื่อพัฒนาและดูแล
งาน จัดทำเว็บไซต์ของบริษัท
ประโยชน์ที่ได้รับ
- เป็นช่องทางในการโฆษณาประชาสัมพันธ์และเปิดตลาดใหม่
- ใช้เป็นแหล่งอ้างอิงจุดเดียวของการให้ข้อมูลของบริษัทและตัวสินค้า ใช้ได้ทั้งสำหรับคู่ค้าและพนักงานในบริษัท
- ใช้ให้บริการหลังการขาย
สิ่งที่ต้องจัดเตรียมเบื้องต้น
- จดทะเบียนโดเมนเนม
- จัดหาเว็บโฮสติ้ง
- สมัครใช้บริการอินเทอร์เน็ต
งาน จัดทำระบบอินทราเน็ต (ไม่จำเป็นสำหรับบริษัท/องค์กรขนาดเล็ก)
ประโยชน์ที่ได้รับ
- ให้บริการด้านข้อมูลที่สำคัญกับพนักงานภายในองค์กรได้สะดวก โดยเฉพาะกับองค์กรที่มีสาขากระจายไปทั่วประเทศ
- ลดขั้นตอนการทำงานภายใน อาทิ การออกจดหมายเวียน ประกาศภายใน
สิ่งที่ต้องจัดเตรียมเบื้องต้น
- Server
- จัดสร้างฐานข้อมูลองค์กร
- การออกแบบระบบที่จะใช้งาน
งาน พัฒนาระบบที่มีความซับซ้อน
- พัฒนาเรื่องข้อมูลที่มีความเคลื่อนไหว สร้างมูลค่าเพิ่มเว็บไซต์เพื่อบริการลูกค้า อาทิ ข่าวสารความเคลื่อนไหวที่จะเป็นประโยชน์ต่อลูกค้า
- การซื้อขาย ชำระเงินผ่านอินเทอร์เน็ต
- ระบบการติดตามการจัดส่งสินค้า
- ระบบห่วงโซ่การผลิต

- ระบบเอ็กซ์ทราเน็ต

ประโยชน์ที่ได้รับ

- เพิ่มประสิทธิภาพการบริการลูกค้า
- เพิ่มศักยภาพในการเข้าสู่ตลาดใหม่ มีโอกาสขายสินค้าสู่ตลาดใหม่ได้มากขึ้น
- ได้รับเงินอย่างรวดเร็ว
- เพิ่มความสัมพันธ์อันดีระหว่างคู่ค้า

สิ่งที่ต้องจัดเตรียมเบื้องต้น

- ให้สิทธิในการเข้าดูฐานข้อมูลแก่คู่ค้า
- อาจต้องลงทุนเรื่อง Server เพิ่มขึ้น
- ต้องลงทุนด้านโปรแกรมและอุปกรณ์เกี่ยวกับการรักษาความปลอดภัยของระบบเพิ่มมากขึ้น

ค่าใช้จ่าย

ตามที่อธิบายไว้ว่าการที่จะเลือกเทคโนโลยีมาใช้นั้นมีตั้งแต่ง่ายๆไปจนถึงระบบที่มีความซับซ้อนมีองค์ประกอบเยอะ ดังนั้นจึงมีค่าใช้จ่ายต่างกันไปด้วย ซึ่งจะแบ่งค่าใช้จ่ายออกเป็น 2 ประเภท คือ

*** ค่าใช้จ่ายขั้นต้น (One-time Costs)**

ค่าใช้จ่ายขั้นต้นจะครอบคลุมค่าใช้จ่ายในด้านต่างๆต่อไปนี้

- ค่าเครื่องคอมพิวเตอร์และอุปกรณ์ที่ใช้ประกอบ โมเด็ม เครื่องพิมพ์ เครื่องพิมพ์บาร์โค้ด เครื่องสแกนบาร์โค้ด
- ค่าอุปกรณ์เครือข่ายในสำนักงาน อาทิ ค่าสาย LAN ค่า HUB
- ค่า Server ที่จะใช้
- ค่าใช้บริการเชื่อมต่ออินเทอร์เน็ต
- ค่าจดทะเบียนโดเมนเนม
- ค่าพัฒนาเว็บไซต์หรือระบบที่ใช้

*** ค่าใช้จ่ายประจำ (Continuous Costs)**

เป็นค่าใช้จ่ายที่ต้องจ่ายตามรอบจะครอบคลุมค่าใช้จ่ายด้านต่างๆดังนี้

- ค่าบำรุงรักษาอุปกรณ์
- ค่าเช่าสายสัญญาณ
- ค่าลิขสิทธิ์ซอฟต์แวร์
- ค่าเปลี่ยนหรืออัพเกรดอุปกรณ์

ความรู้เกี่ยวกับเรื่องความปลอดภัยในระบบคอมพิวเตอร์ที่ควรทราบ

ปัญหาที่ได้รับคะแนนโหวตลำดับต้นๆในการสำรวจเกี่ยวกับการทำพาณิชย์อิเล็กทรอนิกส์คือประเด็นเรื่องไม่มั่นใจในเรื่องความปลอดภัยในระบบอินเทอร์เน็ต เรื่องความปลอดภัยในระบบการชำระเงิน ดังนั้นในหัวข้อนี้จะมาศึกษากันถึงประเด็นดังกล่าวว่าภัยที่ว่ามีอะไรบ้างเราจะป้องกันหรือมีเครื่องมือป้องกันได้อย่างไรบ้าง

มาตรการการรักษาความปลอดภัยของข้อมูล

ระบบรักษาความปลอดภัยของข้อมูลของพาณิชย์อิเล็กทรอนิกส์จึงต้องมีมาตรการดังต่อไปนี้

- การระบุตัวบุคคล และ อำนาจหน้าที่ (Authentication & Authorization) คือ การระบุตัวบุคคลที่ติดต่อว่าเป็นบุคคลตามที่ได้

กล่าวอ้างไว้จริง และ มี อำนาจหน้าที่ตามที่ได้กล่าวอ้างไว้จริง (เปรียบเทียบได้กับการแสดงตัวด้วยบัตรประจำตัวซึ่งมีรูปติดอยู่ด้วย หรือ การใช้ระบบล็อคซึ่งผู้ที่จะเปิดได้จะต้องมีกุญแจอยู่เท่านั้น เป็นต้น)

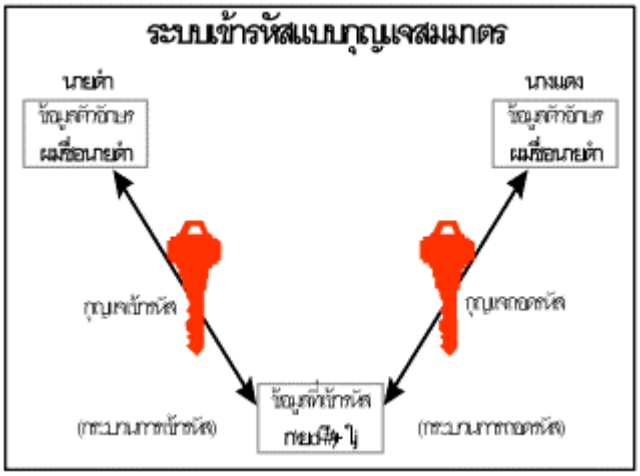
- การรักษาความลับของข้อมูล (Confidentiality) คือ การรักษาความลับของข้อมูลที่เก็บไว้ หรือ ส่งผ่านทางเครือข่ายโดยป้องกันไม่ให้ผู้อื่นที่ไม่มีสิทธิ์ลักลอบดูได้ (เปรียบเทียบได้กับ การปิดผนึกซองจดหมาย การใช้ซองจดหมายที่ทึบแสง การเขียนหมึกที่มองไม่เห็น เป็นต้น)
- การรักษาความถูกต้องของข้อมูล (Integrity) คือ การป้องกันไม่ให้ข้อมูลถูกแก้ไข โดยตรวจสอบไม่ได้ (เปรียบเทียบได้กับ การเขียนด้วยหมึกซึ่งถ้าถูกลบแล้วจะก่อให้เกิดรอยลบขึ้น การใช้โฮโลแกรมกำกับบนบัตรเครดิต เป็นต้น)
- การป้องกันการปฏิเสธ หรือ อ้าง ความรับผิดชอบ (Non-repudiation) คือ การป้องกันการปฏิเสธว่าไม่ได้มีการส่ง หรือ รับข้อมูล จากฝ่ายต่างๆที่เกี่ยวข้อง หรือ การป้องกันการอ้างที่เป็นเท็จว่าได้ รับ หรือ ส่งข้อมูล (เปรียบเทียบได้กับการส่งจดหมายลงทะเบียน เป็นต้น)

<u>เทคโนโลยีในการรักษาความปลอดภัยมีอะไรบ้าง</u>

สำรับพาณิชย์อิเล็กทรอนิกส์นั้นไม่ว่าข้อมูลที่ถูกเก็บไว้ หรือ ที่ถูกส่งผ่านทางเครือข่าย นั้น ล้วนแต่เป็นข้อมูลอิเล็กทรอนิกส์ทั้งสิ้น ซึ่งธรรมชาติของข้อมูลอิเล็กทรอนิกส์นั้นง่ายต่อการเปลี่ยนแปลง หรือ ทำลายโดยไร้ร่องรอย ง่ายต่อการโอนย้ายจากที่หนึ่งไปยังอีกที่หนึ่งโดยเร็ว จึงจำเป็นที่จะต้องอาศัยเทคโนโลยีต่างๆมาเพื่อรักษาความปลอดภัยของข้อมูลให้ได้ตามมาตรการทั้ง 4 ประการข้างต้น และ เนื่องจากระบบ พาณิชย์อิเล็กทรอนิกส์นั้นตัวข้อมูลอิเล็กทรอนิกส์เองนั้นจะถูกเก็บ และ ส่งผ่านในระบบเครือข่าย ประเภทของการรักษาความปลอดภัยของ ข้อมูลแบ่งออกเป็น 2 ประเภทใหญ่ คือ การรักษาความปลอดภัยของการทำธุรกรรม (Transaction Security) และ การรักษาความปลอดภัย ของเครือข่าย (Network Security) เทคโนโลยีการรักษาความปลอดภัยของข้อมูลในการทำธุรกรรม นั้น ได้แก่

การรหัส (Cryptography) คือ การทำให้ข้อมูลที่จะส่งผ่านไปทางเครือข่ายอยู่ในรูปแบบที่ไม่สามารถอ่านออกได้ ด้วยการเข้ารหัส (Encryption) ทำให้ข้อมูลนั้นเป็นความลับ ซึ่งผู้ที่มีสิทธิ์จริงเท่านั้นจะสามารถอ่านข้อมูลนั้นได ด้วยการถอดรหัส (Decryption) นั่นคือ สามารถรักษาข้อมูลให้เป็นความลับ (Confidentiality) และ กำหนดผู้ มีสิทธิ์ได้ (Authentication & Authorization) สำหรับการเข้ารหัส และ ถอดรหัสนั้นจะอาศัยสมการทางคณิตศาสตร์ที่ซับซ้อน และ ต้องอาศัยกุญแจซึ่งอยู่ในรูปของพารามิเตอร์ที่กำหนดไว้ (สำหรับตัวกุญแจนั้นจะมีความยาวเป็น บิต(bit) และ ยิ่งกุญแจมีความยาวมาก ยิ่งปลอดภัยมาก เนื่องจากจะต้องใช้เวลานานมากขึ้นในการ คาดเดากุญแจโดยผู้คุกคาม) ในการเข้า และ ถอดรหัส สามารถแบ่งออกเป็น 2 ประเภท คือ การรหัสแบบกุญแจสมมาตร(Symmetric Key Cryptography หรือ Secret Key Cryptography) และ การรหัสแบบอสมมาตร (Asymmetric Key Cryptography หรือ Public Key Cryptography)

- **การรหัสแบบกุญแจสมมาตร** หมายถึง การเข้า และ ถอดรหัส โดยใช้กุญแจลับที่เหมือนกัน ซึ่งมีขั้นตอนแสดงดังตัวอย่าง ในรูปที่ 1 คือ นายแดงเป็นผู้ส่ง จะทำการส่งผ่านข้อความ "ผมชื่อนายดำ" ไปยัง ผู้รับคือ นางแดง โดยที่ นายดำทำการเข้า รหัสข้อความ "ผมชื่อนายดำ" ด้วยกุญแจลับ ข้อความนั้นจะเปลี่ยนเป็น ข้อความที่เข้ารหัสแล้ว(Cipher Text) "ก\ยd-#)+ใ" ถูกส่งไปยังนางแดง จากนั้นนางแดงก็ใช้กุญแจลับเดียวกันกับที่นายแดงใช้เข้ารหัสมาทำการถอดรหัสออกมาเป็นข้อความเดิมคือ "ผมชื่อนายดำ" ในกรณีนี้กุญแจลับจะเป็นกุญแจเดียวกันซึ่งจะต้องเป็นที่รู้กันเพียงผู้รับและผู้ส่งเท่านั้น
- **การรหัสแบบกุญแจอสมมาตร** หมายถึง การเข้า และ ถอดรหัส ด้วยกุญแจต่างกัน ซึ่งมีขั้นตอนดังตัวอย่างที่แสดงไว้ในรูป คือ นายดำเป็นผู้ส่งทำการเข้ารหัสข้อความ "ผมชื่อนายดำ" ไปเป็น "มt*แ)สp@dะ" ด้วยกุญแจสาธารณะของผู้รับได้แก่ นางแดง ซึ่งนายดำขอกุญแจนั้นมาจากองค์กรกลางที่เก็บกัญแจสาธารณะของบุคคลต่างๆไว้ จากนั้นข้อความที่เข้ารหัสแล้วถูกส่งไปยัง นางแดง นางแดงจะทำการถอดรหัสข้อความด้วยกุญแจส่วนตัวของนางแดง และ นางแดงเท่านั้นจะเป็นผู้มีสิทธิ์ เนื่องจากนางแดงจะเป็นผู้เดียวที่มีกุญแจส่วนตัวของนางแดงเอง นั่นคือ ในการส่งข้อความด้วยการเข้ารหัสแบบกุญแจอสมมาตร จะเน้นที่ผู้รับเป็นหลัก คือ จะใช้กุญแจสาธารณะของผู้รับซึ่งเป็นที่เปิดเผยในการเข้ารหัส และ จะใช้กุญแจส่วนตัวของผู้รับในการถอดรหัส



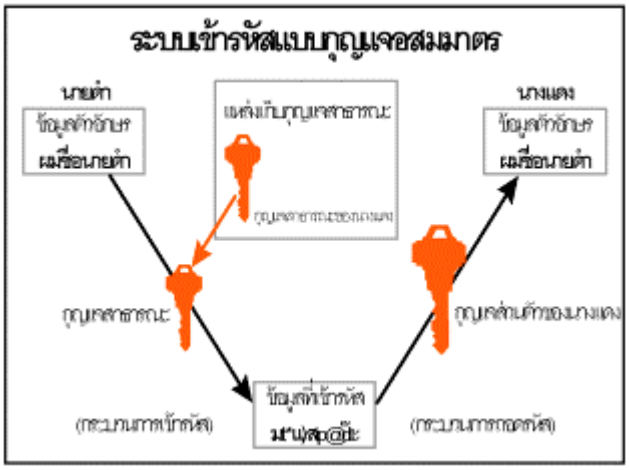
แบบกุญแจสมมาตร

ข้อดี

- มีความรวดเร็ว เพราะใช้การคำนวณที่น้อยกว่า
- สามารถสร้างได้ง่ายโดยใช้ฮาร์ดแวร์

ข้อเสีย

- การบริหารจัดการกุญแจทำได้ยากเพราะ กุญแจในการเข้ารหัส และ ถอดรหัส เหมือนกัน



แบบกุญแจสมมาตร

ข้อดี

- การบริหารจัดการกุญแจทำได้ง่ายกว่า เพราะใช้กุญแจในการเข้ารหัส และถอดรหัสต่างกัน

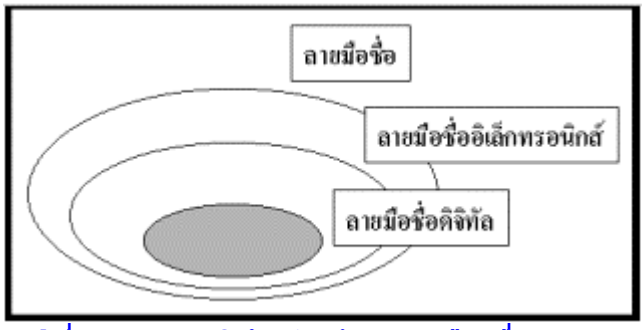
- สามารถระบุผู้ใช้โดยการใช้ร่วมกับลายมือชื่ออิเล็กทรอนิกส์

ข้อเสีย

- ใช้เวลาในการเข้า และ ถอดรหัสค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก

<u>Digital Signature คืออะไร</u>

ในการส่งข้อมูลผ่านเครือข่ายนั้น นอกจากจะทำให้ข้อมูลที่ส่งนั้นเป็นความลับสำหรับผู้ไม่มีสิทธิ์โดยการใช้เทคโนโลยีการรหัส แล้ว สำหรับการทำนิติกรรมสัญญาโดยทั่วไป ลายมือชื่อจะเป็นสิ่งที่ใช้ในการระบุตัวบุคคล (Authentication) และ ยังมีแสดงถึงเจตนาในการยอมรับเนื้อหาในสัญญานั้นๆซึ่งเชื่อมโยงถึง การป้องกันการปฏิเสธความรับผิดชอบ (Non-repudiation) สำหรับในการทำธุรกรรมทางอิเล็กทรอนิกส์นั้นจะใช้ ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature) ซึ่งมีรูปแบบต่างๆเช่น สิ่งที่ระบุตัวบุคคลทางชีวภาพ (ลายพิมพ์นิ้วมือ เสียง ม่านตา เป็นต้น) หรือ จะเป็นสิ่งที่มอบให้แก่บุคคลนั้นๆในรูปแบบของ รหัสประจำตัว ตัวอย่างที่สำคัญของลายมือชื่ออิเล็กทรอนิกส์ที่ได้รับการยอมรับกันมากที่สุดอันหนึ่งคือ ลายมือชื่อดิจิทัล (Digital Signature) ซึ่งจะเป็นองค์ประกอบหนึ่งใน โครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure, PKI)



รูปที่ 1 แสดงให้เห็นถึงลายมือชื่อดิจิทัลเป็นตัวอย่างหนึ่งของลายมือชื่ออิเล็กทรอนิกส์

ลายมือชื่อดิจิทัล (Digital Signature) คือ
ข้อมูลอิเล็กทรอนิกส์ที่ได้จากการเข้ารหัสข้อมูลด้วยกุญแจส่วนตัวของผู้ส่งซึ่งเปรียบเสมือนเป็นลายมือชื่อของผู้ส่ง คุณสมบัติของลายมือชื่อดิจิทัล นอกจากจะสามารถ ระบุตัวบุคคล และ เป็นกลไกการป้องกันการปฏิเสธความรับผิดชอบแล้ว ยังสามารถป้องกันข้อมูลที่ส่งไปไม่ให้ถูกแก้ไข หรือ หากถูกแก้ไขไปจากเดิมก็สามารถล่วงรู้ได้ กระบวนการสร้างและ ลงลายมือชื่อดิจิทัลมีขั้นตอนแสดงดังในรูปที่ 2 คือ

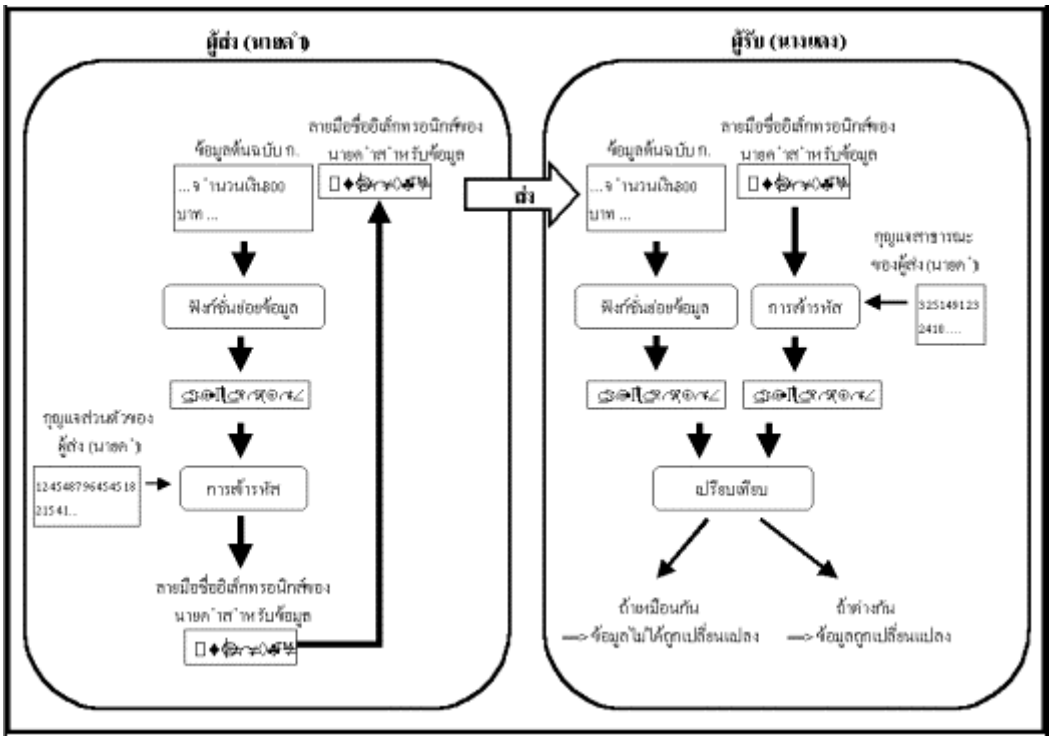
- **เริ่มจากการนำเอาข้อมูลอิเล็กทรนอิกส์ต้นฉบับที่จะส่งไปนั้นมาผ่านกระบวนการทางคณิตศาสตร์ที่เรียกว่า ฟังก์ชันย่อยข้อมูล (Hash Function) เพื่อให้ได้ข้อมูลที่สั้นๆ ที่เรียกว่า ข้อมูลที่ย่อยแล้ว (Digest) ก่อนที่จะทำการเข้ารหัส เนื่องจากข้อมูลต้นฉบับมักจะมีความยาวมาก ซึ่งจะทำให้กระบวนการเข้ารหัสใช้เวลานานมาก**
- **จากนั้นจึงทำการเข้ารหัสด้วยกุญแจส่วนตัวของผู้ส่งเอง ซึ่งจุดนี้เปรียบเสมือนการลงลายมือชื่อของผู้ส่งเพราะผู้ส่งเท่านั้นที่มีกุญแจส่วนตัวของผู้ส่งเอง และ จะได้ข้อมูลที่เข้ารหัสแล้ว เรียกว่า ลายมือชื่อดิจิทัล**
- **จากนั้นก็ทำการส่ง ลายมือชื่อไปพร้อมกับข้อมูลต้นฉบับ ไปยังผู้รับ ผู้รับก็จะทำการตรวจสอบว่าข้อมูลที่ได้รับถูกแก้ไขระหว่างทางหรือไม่ โดยการนำข้อมูลต้นฉบับที่ได้รับ มาผ่านกระบวนการย่อยด้วย ฟังก์ชันย่อยข้อมูล จะได้ข้อมูลที่ย่อยแล้วอันหนึ่ง และ**
- **นำลายมือชื่อดิจิทัล มาทำการถอดรหัสด้วย กุญแจสาธารณะของผู้ส่ง ก็จะได้ข้อมูลที่ย่อยแล้วอีกอันหนึ่ง แล้วทำการเปรียบเทียบ ข้อมูลที่ย่อยแล้วทั้งสองอัน ถ้าหากว่าเหมือนกัน ก็แสดงว่าข้อมูลที่ได้รับนั้นไม่ได้ถูกแก้ไข แต่ถ้าข้อมูลที่ย่อยแล้ว แตกต่างกัน ก็แสดงว่า ข้อมูลที่ได้รับถูกเปลี่ยนแปลงระหว่างทาง**

จากกระบวนการลงลายมือชื่อดิจิทัลข้างต้นมีข้อพึงสังเกตุดังต่อไปนี้

- **ลายมือชื่อดิจิทัลจะแตกต่างกันไปตามข้อมูลต้นฉบับและบุคคลที่จะลงลายมือชื่อ ไม่เหมือนกับลายมือชื่อทั่วไปที่จะต้องเหมือนกันสำหรับบุคคลนั้นๆ ไม่ขึ้นอยู่กับเอกสาร**
- **กระบวนการที่ใช้จะมีลักษณะคล้ายคลึงกับการเข้ารหัสแบบอสมมาตร แต่การเข้ารหัสจะใช้ กุญแจส่วนตัวของผู้ส่ง และ การถอดรหัสจะใช้ กุญแจสาธารณะของผู้ส่ง ซึ่งสลับกันกับ การเข้าและถอดรหัสแบบ กุญแจอสมมาตร ในการรักษาข้อมูลให้เป็นความลับ**

ในรูปที่ 2 แสดงถึงกระบวนการลงลายมือชื่อดิจิทัล แต่ในการใช้งานจริงข้อมูลต้นฉบับที่ส่งไปก็ควรจะถูกเข้ารหัสด้วยเพื่อทำให้ข้อมูลเป็นความลับ

สำหรับผู้ที่ไม่มีสิทธิ์



รูปที่ 2 แผนภาพกระบวนการลงลายมือชื่อดิจิทัล

ใบรับรองดิจิทัล (Digital Certificate)

ด้วยการรหัส และ ลายมือชื่อดิจิทัล ในการทำธุรกรรม เราสามารถ รักษาความลับของข้อมูล สามารถรักษาความถูกต้องของข้อมูล และ สามารถระบุตัวบุคคลได้ระดับหนึ่ง เพื่อเพิ่มระดับความปลอดภัยในการระบุตัวบุคคลโดยสร้างความเชื่อถือมากขึ้นด้วย ใบรับรองดิจิทัล (Digital Certificate) ซึ่งออกโดยองค์กรกลางที่เป็นที่เชื่อถือ เรียกว่า องค์กรรับรองความถูกต้อง (Certification Authority) จะถูกนำมาใช้สำหรับยืนยันในตอนทำธุรกรรมว่าเป็นบุคคลนั้นๆจริง ตามที่ได้อ้างไว้ สำหรับรายละเอียดในใบรับรองดิจิทัลทั่วไปมีดังต่อไปนี้

- ข้อมูลระบุผู้ที่ได้รับการรับรอง ได้แก่ ชื่อ องค์กร ที่อยู่
- ข้อมูลระบุผู้ออกใบรับรอง ได้แก่ ลายมือชื่อดิจิทัลขององค์กรที่ออกใบรับรอง หมายเลขประจำตัวของผู้ออกใบรับรอง
- กุญแจสาธารณะของผู้ที่ได้รับการรับรอง
- วันหมดอายุของใบรับรองดิจิทัล
- ระดับชั้นของใบรับรองดิจิทัล ซึ่งมีทั้งหมด 4 ระดับ ในระดับ 4 จะมีกระบวนการตรวจสอบเข้มงวดที่สุด และ ต้องการข้อมูลมากที่สุด
- หมายเลขประจำตัวของใบรับรองดิจิทัล

ประเภทของใบรับรองดิจิทัลยังแบ่งออกเป็น 3 ประเภท คือ ใบรับรองเครื่องแม่ข่าย ใบรับรองตัวบุคคล ใบรับรองสำหรับองค์รับรองความถูกต้อง

แหล่งที่มา http://www.ecommerce.or.th