

# บทที่ 5-6

- กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล  
(Data Protection Law)
- เทคโนโลยีระบบการรักษาความปลอดภัย



# การคุ้มครองความเป็นส่วนตัว

**ความเป็นส่วนตัว** คือ สิทธิที่อยู่ตามลำพัง เป็นอิสระจากสิ่งภายนอก หรือสิ่งรอบข้างไม่ต้องการเข้าไปข้องเกี่ยวกับเรื่องของคนอื่น หรือองค์กรใด

**ความเป็นส่วนตัวของข้อมูลสารสนเทศ** คือ สิทธิในการตัดสินใจว่าเมื่อใดข้อมูลสารสนเทศของบุคคลหนึ่ง จะสามารถเปิดเผยให้กับผู้อื่นได้ และภายใต้ขอบเขตอย่างไร

- การละเมิดความเป็นส่วนตัวบนโลกอินเทอร์เน็ต  
ทำได้โดยการลักลอบดูข้อมูลส่วนตัวของผู้อื่น ปลอมแปลงเป็นผู้อื่น เป็นต้น
- การกระทำใดๆ บนอินเทอร์เน็ตที่ทำให้บุคคลนั้นๆ  
รู้สึกว่าคุณละเมิดความเป็นส่วนตัว ถือว่าผิดกฎหมายในเกือบทุกประเทศ





# แนวทางการพัฒนากลุ่มรองความเป็นส่วนตัว

## ความถูกต้องแม่นยำของข้อมูล

- ข้อมูลส่วนตัว ควรจะได้รับการตรวจสอบก่อนจะนำเข้าสู่ฐานข้อมูล
- ข้อมูลควรมีความถูกต้องแม่นยำ และมีความทันสมัย
- เพิ่มข้อมูลควรทำให้บุคคลสามารถเข้าถึง (ข้อมูลของตน) และตรวจสอบความถูกต้องได้





# แนวทางการพัฒนาคู่มือรองความเป็นส่วนตัว

## ความลับของข้อมูล

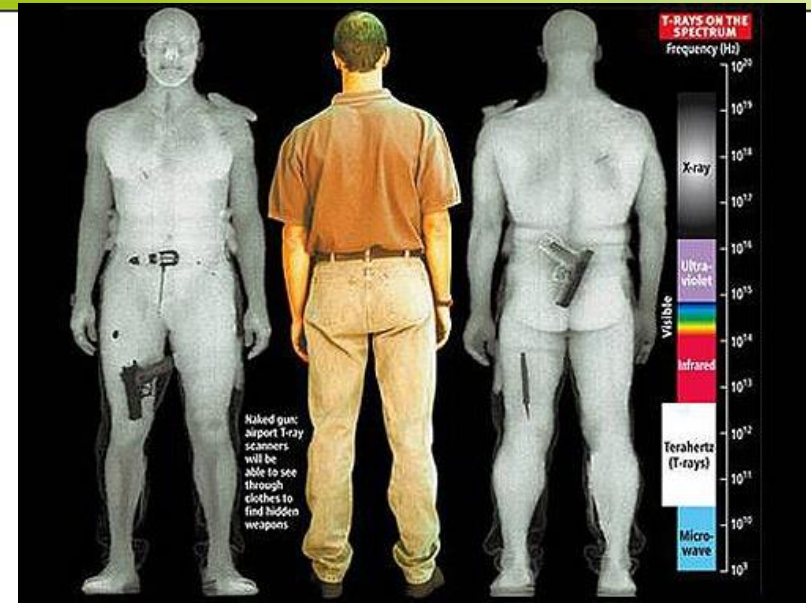
- ควรมีมาตรการป้องกันความปลอดภัยของข้อมูลบุคคล ไม่ว่าจะเป็นทางด้านเทคนิค และการบริหาร
- บุคคลที่สามไม่สมควรได้รับอนุญาตให้เข้าถึงข้อมูลโดยปราศจากการรับรู้หรืออนุญาตของเจ้าของ ยกเว้น โดยข้อกำหนดของกฎหมาย
- ข้อมูลไม่ควรถูกเปิดเผยด้วยเหตุผลที่ไม่ตรงกับวัตถุประสงค์ในการเก็บข้อมูล



# ภัยคุกคามต่อความเป็นส่วนตัวและ ข้อมูลส่วนบุคคล

- Club Cards ของซูเปอร์มาร์เก็ต คือ การที่เจ้าของกิจการได้เก็บข้อมูลส่วนบุคคลของลูกค้า รวมถึงข้อมูลการซื้อของลูกค้าในแต่ละครั้ง นำไปสู่การจัดรายการโปรโมชั่นจูงใจให้ลูกค้ากลับมาซื้ออีก
- เครื่องสแกนร่างกาย เป็นเทคโนโลยีคอมพิวเตอร์ที่ถูกนำไปใช้ในการตรวจหาอาวุธในสนามบิน ซึ่งถูกนำไปใช้ในบริษัทผลิตเสื้อผ้าหลายแห่ง เพื่อให้ลูกค้าได้สวมใส่เสื้อผ้าที่มีขนาดพอดีตัว โดยระบบจะสแกนร่างกายลูกค้า แล้วจำลองเป็นโมเดล 3 มิติ เมื่อลูกค้าต้องการสั่งเสื้อผ้า ระบบจะแนะนำเสื้อผ้าที่มีขนาดตรงกับสัดส่วนของลูกค้า





ตัวอย่างการนำเครื่องสแกน  
ร่างกายไปใช้ในสนามบิน



# ภัยคุกคามต่อความเป็นส่วนตัวและข้อมูลส่วนบุคคล

- กล้องดำในรถยนต์ อยู่ในรูปของ Microprocessor สามารถบันทึกข้อมูลความเร็ว ค่าความดันรถ ก่อนแต่ละเบรก ฯลฯ โดยหากเกิดอุบัติเหตุขึ้น เจ้าหน่อกษัตริย์จะสามารถรวบรวมหลักฐานการเกิดอุบัติเหตุได้ ทำให้ข้อมูลพฤติกรรมการขับขี่รถยนต์ถูกเปิดเผย เป็นข้อมูลสาธารณะไปโดยปริยาย



# ภัยคุกคามต่อความเป็นส่วนตัวและข้อมูลส่วนบุคคล

- **GPS Chip** (Global Positioning System Chip) เป็นระบบระบุตำแหน่งประโยชน์ของระบบ GPS ทำให้ธุรกิจหลายประเภทให้ความสนใจ เพื่อเข้าถึงลูกค้าแบบ Real-Time เพื่อจัดเตรียมบริการเชิงข้อมูลอำนวยความสะดวกแก่ลูกค้า เช่น ธนาคารแจ้งตำแหน่งตู้ ATM ที่ใกล้เคียงกับสถานที่ที่ลูกค้าไป เป็นต้น สามารถสร้างความพึงพอใจให้กับลูกค้า แต่ก็ไม่สามารถรับประกันได้ว่าพนักงานจะไม่เปิดเผยข้อมูลตำแหน่งของลูกค้าให้กับบุคคลอื่น หรือระบบจะป้องกันแฮคเกอร์ได้



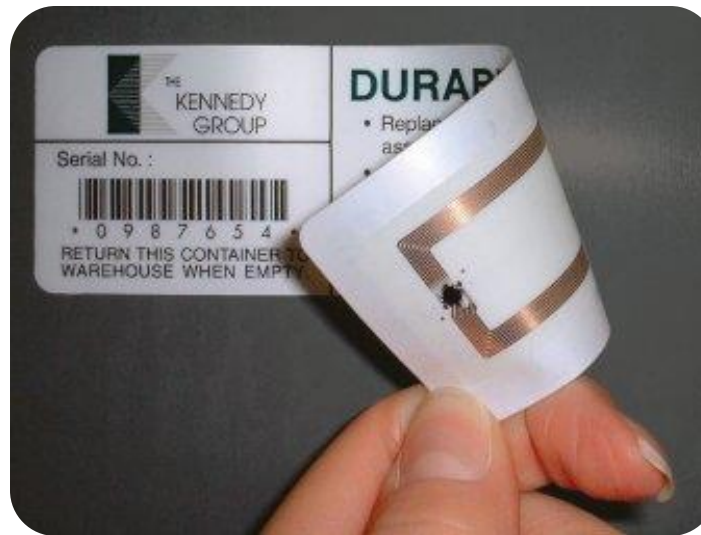


# ภัยคุกคามต่อความเป็นส่วนตัว และข้อมูลส่วนบุคคล

- RFID (Radio Frequency Identification) RFID เป็นแผ่นป้ายอิเล็กทรอนิกส์ที่บรรจุข้อมูลที่เกี่ยวกับการผลิตสินค้าชนิดนั้นเอาไว้ โดยจะฝังหรือติดไว้ที่สินค้า สามารถอ่านค่าภายในโดยใช้อุปกรณ์สำหรับอ่านค่าวิทยุ เพียงแค่ถือเครื่องอ่านผ่านสินค้าภายในระยะ 6 ฟุต โดยรัฐบาลสหรัฐฯ วางแผนจะนำ RFID มาใช้กับหนังสือเดินทาง นำมาพร้อมกับเทคโนโลยีจดจำใบหน้า แต่ในเรื่องความเป็นส่วนตัวหากมีบุคคลอื่นที่ไม่ใช่เจ้าหน้าที่ที่มีอุปกรณ์ที่สามารถอ่านค่าข้อมูลใน RFID ได้ จะทำให้สามารถนำข้อมูลของผู้โดยสารไปใช้ประโยชน์ในทางที่ผิด



# ภัยคุกคามต่อความเป็นส่วนตัวและ ข้อมูลส่วนบุคคล



แสดงตัวอย่างเครื่องอ่าน RFID และแผ่นป้าย RFID

# ผลกระทบของคอมพิวเตอร์ต่อความเป็นส่วนตัว

1. ผลกระทบของต่อความเป็นส่วนตัวในด้านฐานข้อมูล
2. ผลกระทบต่อความเป็นส่วนตัวด้านการใช้เว็บ
3. ผลกระทบต่อความเป็นส่วนตัวด้านไปรษณีย์อิเล็กทรอนิกส์



## A. ผลกระทบของคอมพิวเตอร์ต่อความเป็นส่วนตัว

### ด้านฐานข้อมูล

- 1) ทำให้เกิดการร่วมใช้ข้อมูลร่วมกัน (Sharing Information)
  - สามารถร่วมใช้ข้อมูลร่วมกัน เฉพาะบริษัทสมาชิกที่ต้องทำงานร่วมกัน หรือกับบริษัทภายนอกที่ได้รับอนุญาต
  - ไม่อนุญาตให้บริษัทอื่นๆ มาร่วมใช้ข้อมูลของเรา
- 2) องค์กรอุตสาหกรรมที่มีรูปแบบเฉพาะ  
สามารถควบคุมรูปแบบที่แน่นอนในการใช้ข้อมูลร่วมกันของลูกค้า
- 3) ทำให้เกิดความต้องการอย่างถูกกฎหมาย  
ในรูปแบบที่หลากหลายมากขึ้น ในการอนุญาต หรือการใช้ข้อมูลร่วมกัน
- 4) ทำให้เกิดรูปแบบการเข้ารหัสต่างๆ ขึ้นอยู่กับวิธีการใช้ข้อมูลเหล่านั้นร่วมกัน  
ตามที่ต้องการ อาทิ
  - องค์กรด้านดูแลสุขภาพต้องประสานงานด้านบัญชี กับองค์กรประกันสุขภาพซึ่ง ต้องใช้ข้อมูลร่วมกันด้วย



## ตัวอย่างความเป็นส่วนตัวในด้านฐานข้อมูล (ต่อ)

- บริษัทภายนอกต้องการใช้ข้อมูลร่วมกับองค์กร ด้านดูแลสุขภาพ เพื่อที่จะปฏิบัติการดูแลสุขภาพให้ได้มาตรฐานยิ่งขึ้น
- องค์กรด้านดูแลสุขภาพต้องใช้ข้อมูลผู้ป่วยร่วมกัน กับองค์กรประกันสุขภาพ เพราะต้องประสานงานเรื่องการจ่ายเงินของผู้ป่วย
- องค์กรด้านสุขภาพต้องเข้ารหัส มีส่วนร่วมเพื่อใช้ข้อมูลร่วมกันกับบริษัทภายนอก โดยไม่ให้มีการใช้ข้อมูลผู้ป่วยร่วมกัน





## B. ผลกระทบของคอมพิวเตอร์ต่อความเป็นส่วนตัว

### ด้านการใช้เว็บ

- 1) ทำให้คนที่เข้าใช้เว็บสูญเสียความเป็นส่วนตัว โดยต้องให้ข้อมูลส่วนตัวกับเว็บนั้นก่อน จึงจะได้รับอนุญาตให้เข้าเยี่ยมชมเว็บนั้น ข้อมูลส่วนบุคคลที่มักจะถาม ได้แก่ ชื่อ อายุ ที่อยู่ หมายเลขโทรศัพท์ และ ความชอบส่วนตัว
- 2) เว็บและเครือข่ายทางการตลาดสามารถสร้างแฟ้ม ที่เก็บข้อมูลเกี่ยวกับความสนใจของผู้ใช้ (Profile) จากที่ผู้ใช้ได้เคยให้ข้อมูลไว้ เพื่อจุดประสงค์ในการโฆษณา
- 3) อาจมีการส่งต่อข้อมูลที่ผู้ใช้เคยให้ไว้ เกี่ยวกับเรื่องความสนใจของผู้ใช้ให้กับนักโฆษณา เพื่อเลือกโฆษณาสำหรับผู้ใช้คนนั้น โดยเฉพาะ ให้โฆษณาปรากฏขึ้นที่หน้าจอของผู้ใช้ โดยอัตโนมัติ (Pop Up) เมื่อผู้ใช้เข้าเยี่ยมชมเว็บ



## ความเป็นส่วนตัวด้านการใช้เว็บ (ต่อ)

- 4) อาจมีการส่งโฆษณาทางจดหมายอิเล็กทรอนิกส์ สำหรับผลิตภัณฑ์หรือบริการที่คิดว่า  
ผู้ใช้อาจจะชอบ ซึ่งทำให้เกิดจดหมายขยะ หรือสแปม (Spam)
- 5) ทันทีที่มีการเก็บข้อมูลส่วนตัวของผู้เยี่ยมชมเว็บ ข้อมูลนั้นสามารถให้ผู้อื่นได้ร่วมใช้  
ด้วยและเป็นไปได้ที่อาจมีการใช้ข้อมูลไปในทางที่ผิด
- 6) มีเรื่องเกี่ยวกับนักเจาะระบบที่ได้เข้าถึงเว็บที่มีการรักษาความปลอดภัยอย่างดี  
และได้เจาะเอาข้อมูลหมายเลขบัตรเครดิต และข้อมูลส่วนตัวอื่นๆ
- 7) มีผู้ที่อยู่ภายในองค์กรและมีสิทธิเข้าถึงข้อมูลอย่างถูกต้อง  
อาจกลายเป็นผู้ไม่ซื่อสัตย์และนำข้อมูล ไปใช้ในทางที่ฉ้อฉล



## C. ผลกระทบของคอมพิวเตอร์ต่อความเป็นส่วนตัว

### ด้านความเป็นส่วนตัวอิเล็กทรอนิกส์

1. อาจมีการละเมิดที่อยู่อีเมลส่วนตัวกับเนื้อหาข้อความในอีเมลส่วนตัว เช่น การเก็บ ใช้ และเปิดเผยชื่ออีเมล โดยที่ไม่ได้รับอนุญาตจากเจ้าของ
2. อาจมีข้อความโฆษณาชวนเชื่อที่เราไม่ต้องการส่งมา เรียกว่า ข้อความขยะ หรือสแปม (Spam)
3. อาจมีการนำชื่ออีเมลไปใช้ในทางฉ้อฉล หรือเกี่ยวข้องกับอาชญากรรม
4. อาจมีการเก็บข้อมูลส่วนตัวจากชื่ออีเมล
5. เพียงเราคลิกที่ลิงค์ข้อความ ก็อาจนำไปสู่การลงทะเบียนและการเข้าถึงชื่ออีเมล และข้อมูลส่วนตัวของผู้กดได้



## ความเป็นส่วนตัวด้านอีเมล (ต่อ)

- 6) ชื่ออีเมลและข้อมูลส่วนตัว สามารถตีราคาเป็นเงินได้  
เพราะอาจถูกขายครั้งแล้วครั้งเล่าทั่วโลกโดยที่ไม่ได้รับอนุญาตจากเจ้าของ  
ซึ่งส่งผลให้เกิดสแปมมากขึ้นด้วย
- 7) เรื่องใหม่ที่รุนแรงทางอีเมลคือ “ฟิชซิง (Phishing)”  
เป็นศิลปะการหลอ โกง โดยส่งอีเมล ที่หลอกว่ามาจากบริษัทที่มีชื่อเสียง
- 8) การละเมิดความเป็นส่วนตัว อาจมาจากเมื่อใครคนอื่นล่วงรู้ชื่อ และรหัสผ่าน  
ที่สามารถจะเข้าไปดูอีเมลเราได้
- 9) คนอื่นอาจจะอ่านข้อความในอีเมลของเราได้โดยเราไม่รู้ตัวเป็นปี



# ฟิชซิง (Phishing) (ต่อ)

คือการหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญเช่น รหัสผ่าน หรือ หมายเลขบัตรเครดิต

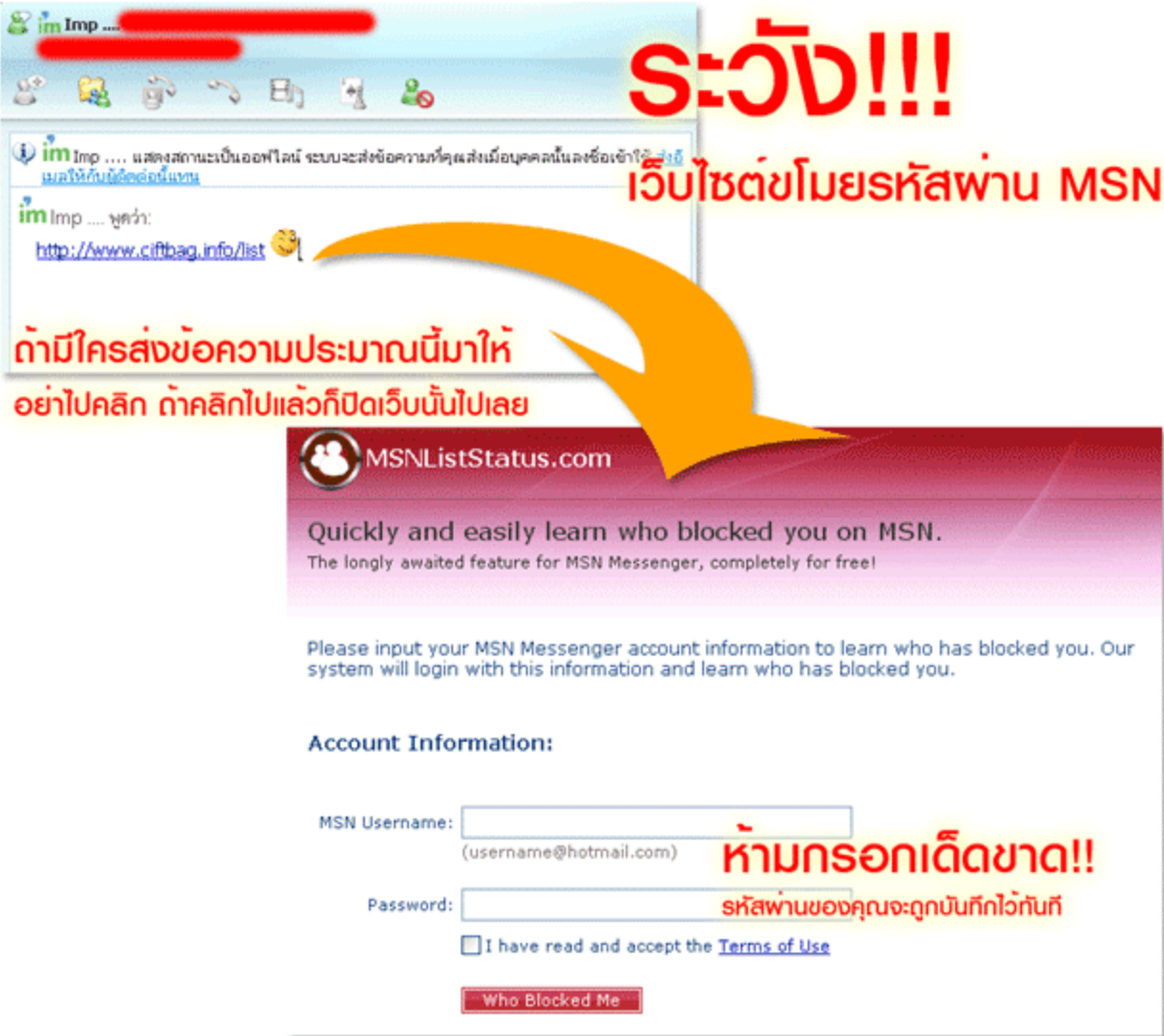
- การโจรกรรมรหัส และอีเมลต้นแบบอื่นๆ
- ข้อมูลจากบริษัทจะระบุถึงปัญหากับเลขบัญชีของผู้รับ และถามเลขบัญชีและข้อมูลส่วนตัวอื่นๆ อ้างว่าเพื่อจะทำแฟ้มข้อมูลให้ถูกต้องแต่นำข้อมูลนี้ไปใช้ในทางฉ้อโกง





**ระวัง!!!**  
เว็บไซต์มอสรหัสผ่าน MSN

ถ้ามีใครส่งข้อความประมาณนี้มาให้  
อย่าไปคลิก ถ้าคลิกไปแล้วก็ปิดเว็บนั้นไปเลย



MSNListStatus.com

Quickly and easily learn who blocked you on MSN.  
The longly awaited feature for MSN Messenger, completely for free!

Please input your MSN Messenger account information to learn who has blocked you. Our system will login with this information and learn who has blocked you.

Account Information:

MSN Username:   
(username@hotmail.com)

Password:

☐ I have read and accept the [Terms of Use](#)

ห้ามกรอกเด็ดขาด!!  
รหัสผ่านของคุณจะถูกบันทึกไว้ทันที

จาก [www.FocusShot.com](http://www.FocusShot.com) เว็บไซต์ข้อมูลกล้องดิจิทัล

- การขโมยข้อมูลเอกลักษณ์บุคคลโดยใช้วิธีการ Phishing

# การขโมยข้อมูลเอกลักษณ์บุคคล

- ข้อมูลที่ใช้แสดงเอกลักษณ์บุคคล เช่น ชื่อ ที่อยู่ วันเดือนปีเกิด หมายเลขใบขับขี่ ฯลฯ ปัจจุบันพบว่ามีฉ้อฉลนิยมใช้ในการขโมยข้อมูลเอกลักษณ์ของบุคคลมี 2 วิธีคือ
- 1. Phishing เป็นการหลอกให้ผู้ใช้ป้อนข้อมูลสำคัญลงในเว็บไซต์ปลอมที่สร้างขึ้นเพื่อหลอกให้ผู้ใช้คลิกเข้าไปป้อนข้อมูลดังกล่าว
- 2. Spyware เป็นโปรแกรมที่ใช้วิธีแฝงตัวในรูปแบบต่างๆ เพื่อหลอกให้ผู้ใช้ดาวน์โหลดไปติดตั้ง โดยหากเป็น spyware ประเภทขโมยข้อมูลส่วนใหญ่จะติดตั้งโปรแกรมที่เรียกว่า “Keystroke-Logging” ลงในเครื่องผู้ใช้โดยไม่รู้ตัว เพื่อบันทึกการป้อนข้อมูลต่างๆ ของผู้ใช้ และจะส่งข้อมูลไปยังผู้สร้าง



# กฎหมายคุ้มครองข้อมูลส่วนบุคคล

☀️ ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540

## มาตรา 34

“สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง การกล่าวหาหรือให้ข่าวแพร่หลายซึ่งข้อความหรือภาพ ไม่ว่าด้วยวิธีใดไปยังสาธารณะอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคล ในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว จะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ”



# หลักการเบื้องต้นของการคุ้มครอง

## 1 การรวบรวมและการจัดเก็บ

- ห้ามไม่ให้จัดเก็บไว้เพื่อเผยแพร่
- ห้ามไม่ให้จัดเก็บข้อมูลที่ได้มาอย่างไม่ถูกต้อง
- ผู้เก็บข้อมูลต้องสื่อถึงเจตนาในการเก็บข้อมูล

## 2 การใช้ข้อมูลส่วนบุคคล

- ต้องเป็นไปตามข้อตกลง
- ถ้าละเมิดต้องมีการตราบทลงโทษเพื่อคุ้มครอง

## 3 การเปิดเผยและการเผยแพร่ข้อมูล

- ห้ามเปิดเผยหรือเผยแพร่เว้นแต่ได้รับความยินยอมจากเจ้าของ



# หลักการเบื้องต้นของการคุ้มครอง

## 4 การกำหนดความรับผิดชอบ

- ผู้รวบรวมต้องตรวจสอบความถูกต้อง
- ต้องปรับปรุงข้อมูลให้ทันสมัย
- ต้องเก็บข้อมูลไว้ในที่ปลอดภัย

## 5 การกำหนดสิทธิของเจ้าของ

- เจ้าของมีสิทธิตรวจสอบข้อมูลของตน
- มีสิทธิปฏิเสธการให้ข้อมูลแก่บุคคลที่สาม

## 6 การคุ้มครองเจ้าของที่ไม่บรรลุนิติภาวะ

- ต้องเก็บข้อมูลโดยตรงจากผู้เยาว์
- ต้องใช้ภาษาง่ายและไม่สับสน
- ผู้ปกครองมีสิทธิ์ที่จะตรวจสอบความถูกต้อง
- ผู้ปกครองมีสิทธิ์ลบทิ้ง ขอให้แก้ไขข้อมูล





# กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Law)

## ■ ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

(1) ความเป็นมา ..... มีการศึกษาและพิจารณาร่างตามแนวทางข้อบังคับของสหภาพยุโรป (EU) โดยเน้นที่ประเทศอิตาลีเป็นหลัก

สาระสำคัญของ **ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล** ยกร่างขึ้นในร่างแรก ๆ โดยอาศัยแนวทางขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic Cooperation and Development) หรือ OECD และ Directive ปัจจุบัน ได้ผ่านความเห็นชอบของ **คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ เมื่อวันที่ ๓ ตุลาคม ๒๕๔๔**

## ■ การให้ความคุ้มครองสิทธิส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลฯ โดย

-- > พรบ.ข้อมูลข่าวสารของทางราชการฯ พศ. ๒๕๔๐



# ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

## (1) ความเป็นมา (ต่อ)

- สถานะปัจจุบันของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล คือ อยู่ในระหว่าง การดำเนินการของคณะทำงานเพื่อศึกษาประเด็นปัญหากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
- หลักสำคัญประการหนึ่ง คือบทบัญญัติว่าด้วยเรื่องการส่งข้อมูลส่วนบุคคลระหว่าง ประเทศ กำหนดว่าการแลกเปลี่ยนข้อมูลจะดำเนินการได้เฉพาะระหว่างประเทศที่มี กฎหมายหรือมีมาตรการในการให้ความคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐาน เพียงพอ กฎเกณฑ์



# ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

## (1) ความเป็นมา (ต่อ)

### (2) ความจำเป็นในการออก กม. ข้อมูลส่วนบุคคลไทย

- เพื่อวางนโยบาย และดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล
- กำหนดการให้ความคุ้มครองข้อมูลส่วนบุคคล

สามารถประมวลผล และเผยแพร่ถึงบุคคล

จำนวนมากได้รวดเร็ว โดยอาศัยเทคโนโลยีสารสนเทศ



# ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

## (1) ความเป็นมา (ต่อ)

### (3) สาระสำคัญของกม. คุ้มครองข้อมูลส่วนบุคคลไทย

#### ● เจตนารมณ์ของกฎหมาย

- ให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นส่วนหนึ่งของสิทธิความเป็นส่วนตัว
- ปัจจุบันมีการละเมิดข้อมูลส่วนบุคคลได้ง่าย สะดวกและรวดเร็วขึ้น

#### ● การประกาศใช้บังคับ (มาตรา 2)

- บังคับใช้เมื่อพ้นกำหนดร้อยแปดสิบวัน (180 วัน) นับแต่วันประกาศในราชกิจจานุเบกษา



### (3) สาระสำคัญของกม. คุ้มครองข้อมูลส่วนบุคคลไทย (ต่อ)

#### ● ขอบเขตของกฎหมาย (มาตรา 3)

- ประชาชนทุกคนจะได้รับการคุ้มครอง ข้อมูลส่วนบุคคลตามหลักเกณฑ์ที่กฎหมายฉบับนี้บัญญัติไว้
- ยกเว้นในกรณีที่มีกฎหมายอื่นเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่มีความเป็นธรรมและมีมาตรฐานมากกว่าให้ใช้ฉบับนั้น

#### ● บทนิยามที่สำคัญ (มาตรา 4)

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ให้คำนิยามของ “ข้อมูลส่วนบุคคล” ที่จะได้รับความคุ้มครองไว้ว่า “หมายความว่า **ข้อเท็จจริงเกี่ยวกับบุคคล** ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม”



**ประมวลจริยธรรม** คือ กฎเกณฑ์และแนวปฏิบัติ เกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งทำเป็นหนังสือ



# สาระสำคัญของกม.คุ้มครองข้อมูลส่วนบุคคลไทย (ต่อ)

## ● ผู้รักษากฎหมาย (มาตรา 5)

- กำหนดให้นายกรัฐมนตรีเป็นผู้รักษาการตามกฎหมายเนื่องจาก
  - \* เกี่ยวข้องกับทุกกระทรวง ทบวง กรม
  - \* มีผลต่อการพัฒนาซึ่งเป็นประโยชน์ ต่อประชาชนโดยรวมทั้งประเทศ

## ● หลักการของกฎหมาย

### (1) บุคคลที่กฎหมายให้ความคุ้มครอง

- กฎหมายให้ความคุ้มครองข้อมูลส่วนบุคคล ของบุคคลธรรมดาเป็นหลัก รวมถึงบุคคลที่เสียชีวิต

### (2) ประเภทของข้อมูลส่วนบุคคล

- ไม่มีการแบ่งประเภทไว้ชัดเจนตามคำจำกัดความ
- แบ่งตามระดับข้อมูลที่ได้รับการคุ้มครองโดยใช้กลไกของกฎหมาย
- การแบ่งประเภทตามค่านิยามอาจทำให้เกิดปัญหาเพราะอาจไม่ครอบคลุม



## หลักการของกม. กลุ่มครองข้อมูลส่วนบุคคลไทย (ต่อ)

### (3) วิธีที่กฎหมายให้ความคุ้มครอง

- ให้ความคุ้มครองกับข้อมูลส่วนบุคคลทั้งทาง อิเล็กทรอนิกส์ (Electronic Means) และที่ทำด้วยมือ (Manual)
- การให้ความคุ้มครองระบบที่ทำด้วยมือ จะให้เฉพาะเท่าที่จำเป็น



# สาระสำคัญของกม.คุ้มครองข้อมูลส่วนบุคคลไทย (ต่อ)

## ● การให้ความคุ้มครองข้อมูลส่วนบุคคล (มาตรา 6-17)

### (1) การวางหลักทั่วไปในการให้ความคุ้มครองข้อมูลส่วนบุคคล

- การดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลจะกระทำมิได้ เว้นแต่เป็นไปตามที่กฎหมายนี้ หรือกฎหมายอื่นบัญญัติไว้

### (2) หลักการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล

- มีการกำหนดหลักเกณฑ์ในการเก็บรวบรวม การใช้ การเปิดเผย การเก็บรักษา และการเข้าถึงข้อมูลส่วนบุคคลไว้แยกจากกัน เพื่อให้เกิดความชัดเจน

### (3) คุ้มครองข้อมูลที่กระทบความรู้สึกรักของประชาชน อาทิ

1) ข้อมูลเกี่ยวกับเชื้อชาติ

2) ข้อมูลเกี่ยวกับเผ่าพันธุ์

3) ความเชื่อทางศาสนา

เป็นต้น

### (4) งานส่งหรือโอนข้อมูล - กำหนดเกี่ยวกับหลักเกณฑ์การส่งหรือโอนข้อมูล



# สาระสำคัญของกม.คุ้มครองข้อมูลส่วนบุคคลไทย (ต่อ)

## ● ประมวลจริยธรรมในการคุ้มครองข้อมูลส่วนตัว

- วางหลักเกณฑ์เพื่อให้ภาคเอกชนสร้างกลไกให้ความคุ้มครองข้อมูลส่วนบุคคลของตนเอง เพื่อให้สอดคล้องกับแนวปฏิบัติเดิม

## ● คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 22-40)

- กำหนดให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- มีหน้าที่กำกับดูแลการปฏิบัติตามกฎหมายและประมวลจริยธรรมที่ภาคเอกชนกำหนด

1. กำหนดนโยบาย

2. วางหลักเกณฑ์ และแนวปฏิบัติต่างๆ

3. การวินิจฉัยข้อพิพาท

- การรับเรื่องร้องเรียนและการอุทธรณ์ การละเมิดข้อมูลส่วนบุคคล

- ส่งเสริมให้ภาคเอกชนจัดทำประมวลจริยธรรมของตนเอง



# สรุป

1) แนวทางการพัฒนาการคุ้มครองความเป็นส่วนตัว

2) ผลกระทบของคอมพิวเตอร์ต่อความเป็นส่วนตัว อาทิ

- ผลกระทบของต่อความเป็นส่วนตัวในด้านฐานข้อมูล
- ผลกระทบต่อความเป็นส่วนตัวด้านการใช้เว็บ
- ผลกระทบต่อความเป็นส่วนตัวด้านไปรษณีย์อิเล็กทรอนิกส์

3) กฎหมายคุ้มครองข้อมูลส่วนบุคคล



# กฎหมายคุ้มครองความเป็นส่วนตัวและ ข้อมูลส่วนบุคคลในประเทศไทย

- “รัฐธรรมนูญแห่งราชอาณาจักรไทย” หมวดที่ 3 “สิทธิและเสรีภาพของชนชาวไทย” ส่วนที่ 3 “สิทธิและเสรีภาพส่วนบุคคล” ดังนี้
- มาตรา 32 บุคคลย่อมมีสิทธิและเสรีภาพในชีวิตและร่างกาย
- มาตรา 33 บุคคลย่อมมีเสรีภาพในเคหสถาน
- มาตรา 34 บุคคลย่อมมีเสรีภาพในการเดินทางและมีเสรีภาพในการเลือกถิ่นที่อยู่ภายในราชอาณาจักร
- มาตรา 35 สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง
- มาตรา 36 บุคคลย่อมมีเสรีภาพในการสื่อสารถึงกันโดยทางที่ชอบด้วยกฎหมาย



# กฎหมายคุ้มครองความเป็นส่วนตัวและ ข้อมูลส่วนบุคคลในประเทศไทย

- **มาตรา 37** บุคคลย่อมมีเสรีภาพบริบูรณ์ในการถือศาสนา นิกายของศาสนา หรือลัทธินิยมในทางศาสนา และย่อมมีเสรีภาพในการปฏิบัติตามศาสนธรรม ศาสนบัญญัติ หรือปฏิบัติ พิธีกรรมตามความเชื่อถือของตน เมื่อไม่เป็นปฏิปักษ์ต่อหน้าที่ของพลเมืองและไม่เป็น การขัดต่อ ความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
- **มาตรา 38** การเกณฑ์แรงงานจะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามบทบัญญัติ แห่งกฎหมาย เฉพาะเพื่อประโยชน์ในการป้องกันภัยพิบัติสาธารณะ อันมีมา เป็นการฉุกเฉิน หรือโดย อาศัยอำนาจตามบทบัญญัติแห่งกฎหมายซึ่งให้กระทำได้ในระหว่างเวลาที่ประเทศอยู่ในภาวะสงคราม หรือการรบ หรือในระหว่างเวลาที่มีประกาศสถานการณ์ฉุกเฉินหรือประกาศใช้กฎอัยการศึก

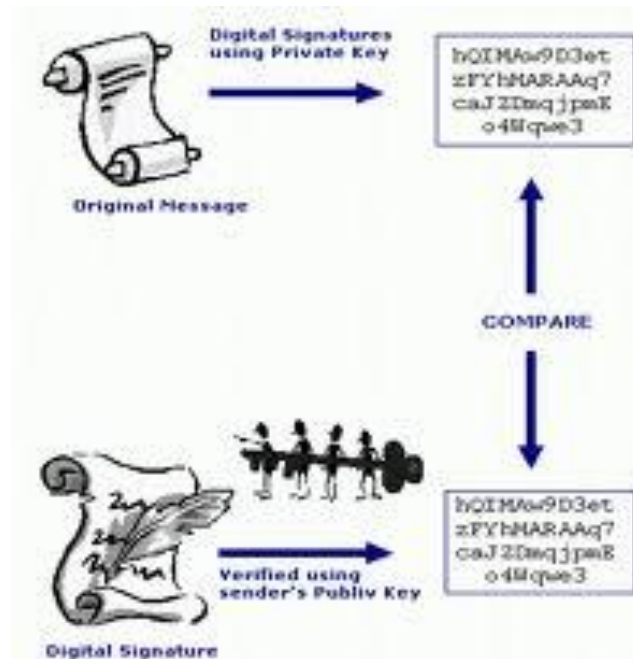
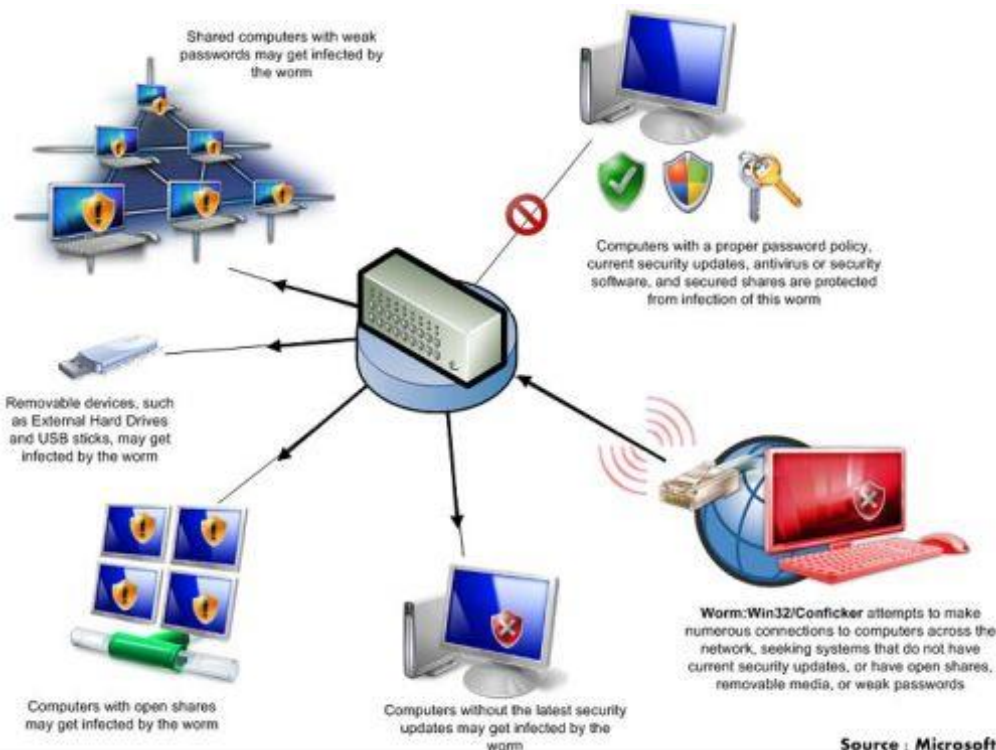
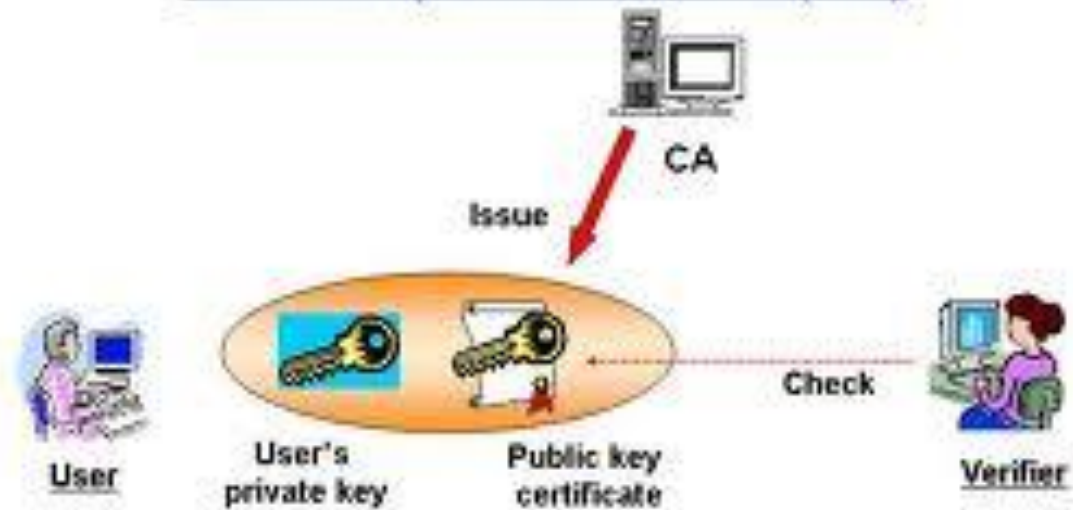
The background of the slide features three bright green apples. One apple is in the foreground, slightly to the right, with its stem visible. Behind it and to the left are two more apples. In the upper right corner, there is a small icon of a key with a yellow shaft and a silver ring.

# บทที่ 6

เทคโนโลยีระบบการรักษาความปลอดภัย

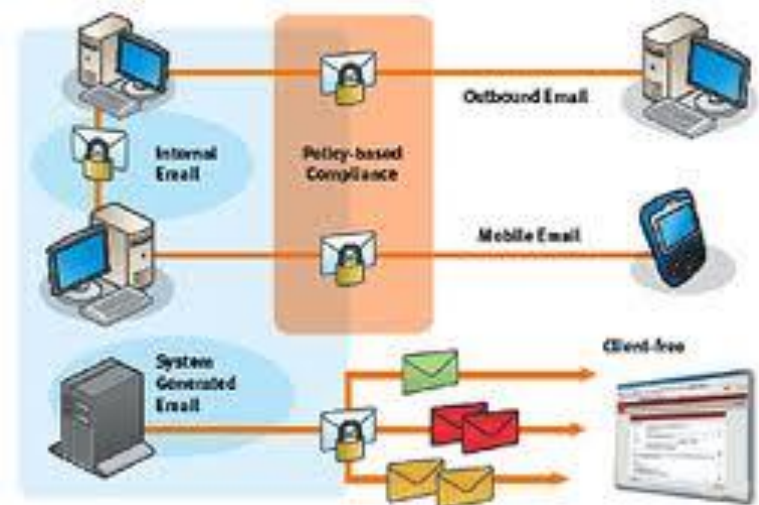
# ตัวอย่างโครงสร้าง

## Public Key Infrastructure (PKI)



# เทคโนโลยีระบบการรักษาความปลอดภัย

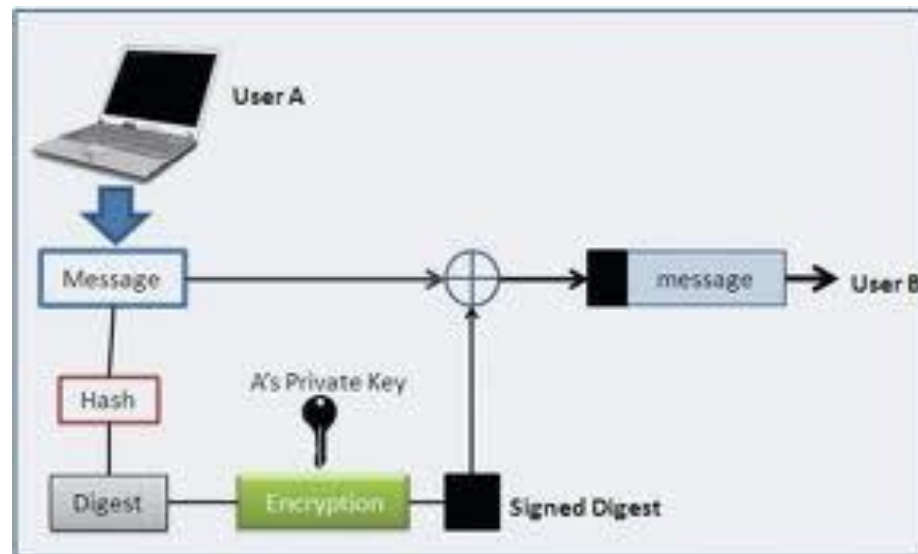
- เทคโนโลยีระบบการรักษาความปลอดภัยมีการนำเอาระบบ **Public Key Infrastructure – PKI** หรือโครงสร้างพื้นฐานของระบบกุญแจสาธารณะมาใช้งาน ซึ่งเป็นเทคโนโลยีที่ได้รับการพิสูจน์และยอมรับโดยทั่วไปว่ามีความปลอดภัยสูง ทำให้การใช้งานระบบพาณิชย์อิเล็กทรอนิกส์มีความน่าเชื่อถือและเกิดความมั่นใจในการใช้งาน





# เทคโนโลยีความปลอดภัยของข้อมูลส่วนบุคคล

- การเข้ารหัสข้อมูล (Encryption) เป็นวิธีป้องกันข้อมูลจากการโจรกรรมในขณะที่มีการรับและส่งข้อมูลผ่านทางเครือข่าย โดยข้อมูลทั้งหมดจะถูกแปลงเป็นรหัสที่ไม่สามารถอ่านได้โดยวิธีปกติ เรียกว่า การเข้ารหัส (Encryption) ดังนั้นแม้จะมีการโจรกรรมข้อมูลไปได้ แต่หากไม่สามารถถอดรหัส (Decryption) ก็ไม่สามารถเข้าใจข้อมูลเหล่านั้นได้



# การรักษาความปลอดภัยให้กับเครือข่ายองค์กร

การป้องกันไม่ให้บุคคลภายนอกสามารถเข้ามาภายในเครือข่ายขององค์กรได้ มี 4 วิธี

1. การควบคุมการเข้าถึงทางกายภาพ (Physical Access Control)
2. การควบคุมการเข้าถึงทางตรรกะ (Logical Access Control)
3. การตรวจสอบการเข้าสู่เครือข่ายโดยไม่ได้รับอนุญาต (Detecting Unauthorized Access)
4. การป้องกันภัยคุกคามจากไวรัส (Virus Protection)





# กิจกรรมส่งในคาบ

## การรักษาความปลอดภัยให้กับเครือข่ายองค์กร

ให้นักศึกษาบอกวิธี การป้องกันไม่ให้บุคคลภายนอกสามารถเข้ามาภายในเครือข่ายขององค์กรได้ (ประเด็นละ 3 ตัวอย่าง)

1. การควบคุมการเข้าถึงทางกายภาพ (Physical Access Control)
2. การควบคุมการเข้าถึงทางตรรกะ (Logical Access Control)
3. การป้องกันภัยคุกคามจากไวรัส (Virus Protection)



# การควบคุมการเข้าถึงทางกายภาพ (Physical Access Control)

- การรักษาความปลอดภัยให้กับสถานที่ปฏิบัติงานเพื่อป้องกันไม่ให้บุคคลที่ไม่พึงประสงค์เข้าไปได้
- ติดตั้งเครื่องรูดบัตรเข้า-ออก
- ติดตั้งโทรทัศน์วงจรปิด
- ติดตั้งระบบดับเพลิง
- รักษาความปลอดภัย HUB, SWITCH



# การควบคุมการเข้าถึงทางกายภาพ

## (Physical Access Control)

### ● Biometrics

- ใช้ลักษณะเฉพาะตัวบุคคลที่แตกต่างกันไปในการตรวจสอบ
- ลายนิ้วมือ
- เสียง
- เรตินา
- ลายเซ็น
- อุณหภูมิ





Multi-Biometric Fusion  
Technology (MBFT) ที่เป็น  
นวัตกรรมใหม่ในการประมวล  
ลายนิ้วมือจาก Sensor หลายตัวได้



Biometric, RFID  
Smartcard Platform

# การควบคุมการเข้าถึงทางตรรกะ (Logical Access Control)

- การรักษาความปลอดภัยให้กับองค์กรจากบุคคลที่ไม่พึงประสงค์ที่ต้องการจะเข้ามายังเครือข่ายขององค์กรโดยการใช้ข้อมูลเฉพาะตัวบุคคล แบ่งเป็น 3 ระดับ
  - Possession การใช้ข้อมูลพิสูจน์ความเป็นเจ้าของ เช่น บัตรประจำตัวต้องมีรูปเจ้าของบัตร
  - Knowledge การนำความรู้มาเป็นส่วนประกอบในการพิสูจน์ตัวบุคคล เช่น id, password
  - Trait การนำลักษณะเฉพาะของบุคคล เช่น ลายนิ้วมือ เรตินา มาใช้ในการพิสูจน์ตัวบุคคล





- การสแกนลายนิ้วมือเป็นเทคโนโลยีที่ได้รับความนิยมมากที่สุดในตอนนี้ เพราะมีราคาถูก ใช้งาน และดูแลไม่เป็นอันตราย
- ข้อดีของการสแกนลายเส้นเลือดที่ฝ่ามือ คือ การสแกนได้โดยไม่ต้องสัมผัส กับอุปกรณ์สแกน แต่ข้อเสียที่มีในอดีตคือ ตัวเซนเซอร์มีขนาดใหญ่ เกินกว่าจะติดตั้งในโน้ตบุ๊กหรือสมาร์ทโฟนได้ อีกทั้งยังมีปัญหาเรื่องไม่สามารถตรวจจับ เมื่อมีการเคลื่อนไหวฝ่ามือ ทำให้สแกนไม่สำเร็จอีกด้วย





# การควบคุมการเข้าถึงทางตรรกะ(Logical Access Control)

- วิธีการควบคุมการเข้าถึงทางตรรกะ
- การเก็บประวัติส่วนตัวของผู้ใช้ (User Profile)
  - id
  - password
  - สิทธิในการทำงานในระดับต่างๆ
  - บางครั้งมีความไม่ปลอดภัยจึงควรเปลี่ยนรหัสบ่อยๆ และกำหนดกฎเกณฑ์ในการตั้งรหัสผ่าน



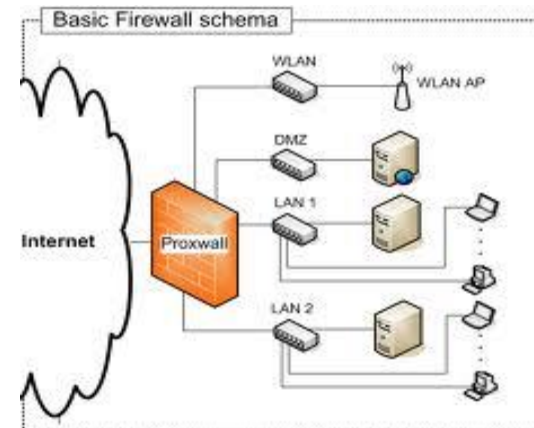
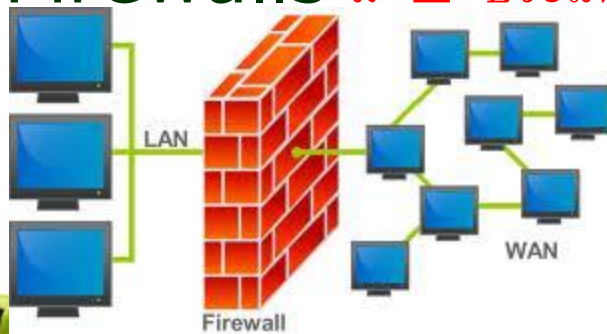


# การควบคุมการเข้าถึงทางตรรกะ(Logical Access Control)

## ● Firewalls

- เป็นโปรแกรมคอมพิวเตอร์ประเภทหนึ่ง ที่นำมาติดตั้งบนเครื่องคอมพิวเตอร์ หรือ **router** ที่มีหน้าที่จัดการและควบคุมการเชื่อมต่อจากภายนอกสู่ภายในองค์กร โดยดูรายละเอียดของตัวควบคุมข้อมูลว่าควรให้ผ่านหรือไม่

## ● Firewalls มี 2 ประเภท



# การควบคุมการเข้าถึงทางตรรกะ (Logical Access Control)

## ● Packet Filtering Firewall

- ตรวจสอบหมายเลข **IP** ต้นทาง ว่าเป็นของเครื่องที่ได้รับอนุญาตในการเข้าสู่ระบบหรือไม่
- ขู่เสี่ย **Hacker** อาจปลอม **IP** เพื่อเข้าสู่ระบบได้

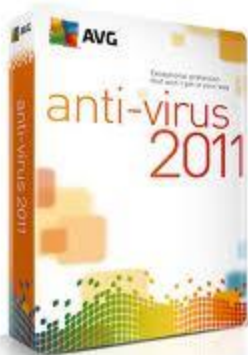
## ● Application Proxy Firewall

- เป็นตัวกลางระหว่างหน่วยงานภายในและภายนอกองค์กร ทำให้องค์กรภายนอกไม่สามารถเข้าสู่ระบบได้ นอกจากนี้ยังสามารถสร้าง **IP** ปลอมเพื่อไม่ให้องค์กรภายนอกทราบ **IP** ที่แท้จริงขององค์กร



# การตรวจสอบการเข้าสู่เครือข่ายโดยไม่ได้รับอนุญาต (Detecting Unauthorized Access)

- การตรวจสอบการทำงานของงาน (Audit Logs)
  - เก็บรายละเอียดประวัติ และพฤติกรรมการใช้ระบบของบุคลากรในองค์กร
- การสร้าง Server ลวง (Entrapment)
  - สร้าง Server ลวงขึ้นมาเพื่อเก็บข้อมูลที่ไม่ใช่ประโยชน์ในองค์กร เพื่อหลอกล่อ Hacker ให้เข้าเจาะระบบ Server ลวง เพื่อจะไถ่ความสนใจจาก Server จริง



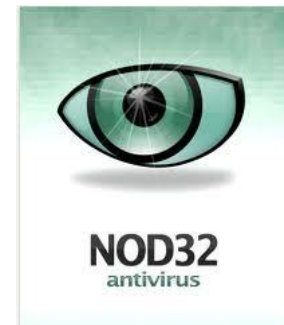
# การป้องกันภัยคุกคามจากไวรัส (Virus Protection)

- ติดตั้งโปรแกรม Scan Virus

- McAfee

- Norton ...

- ติดตั้ง Anti Virus Card



# การรักษาความปลอดภัยในการส่งข้อมูลผ่าน เครือข่ายอินเทอร์เน็ต

- การเข้ารหัส (Encryption)
  - เป็นวิธีการแปลงข้อมูลเป็นรหัส เพื่อไม่ให้ผู้อื่นอ่านได้โดยวิธีการปกติ
- มี 2 วิธี คือ
  - การเข้ารหัสแบบทางเดียว (One-Way Encrytion)
  - การเข้ารหัสแบบสองทาง (Two-Way Encrytion)



# เทคโนโลยีระบบการรักษาความปลอดภัย

- เทคโนโลยี PKI สามารถก่อให้เกิดความน่าเชื่อถือในการระบุตัวตนระหว่างโลกแห่งความจริง (Real World) และโลกอิเล็กทรอนิกส์ (Cyber World) ได้
- โดยใช้เทคโนโลยีระบบรหัสแบบกุญแจสาธารณะ (Public Key Cryptography) ซึ่งประกอบด้วยกุญแจ (Key) 2 ดอก ได้แก่
  - **กุญแจส่วนตัว (Private Key)**
  - **กุญแจสาธารณะ (Public Key)**
- บุคคลหนึ่งๆ จะถือกุญแจคนละ 2 ดอกดังกล่าวนี้นี้ กุญแจส่วนตัวจะถูกเก็บอยู่กับเจ้าของกุญแจไว้อย่างปลอดภัย เพื่อใช้ในการยืนยันตัวตน และกุญแจสาธารณะจะถูกนำไปเผยแพร่ เพื่อให้บุคคลอื่นสามารถติดต่อสื่อสารกับเจ้าของกุญแจได้





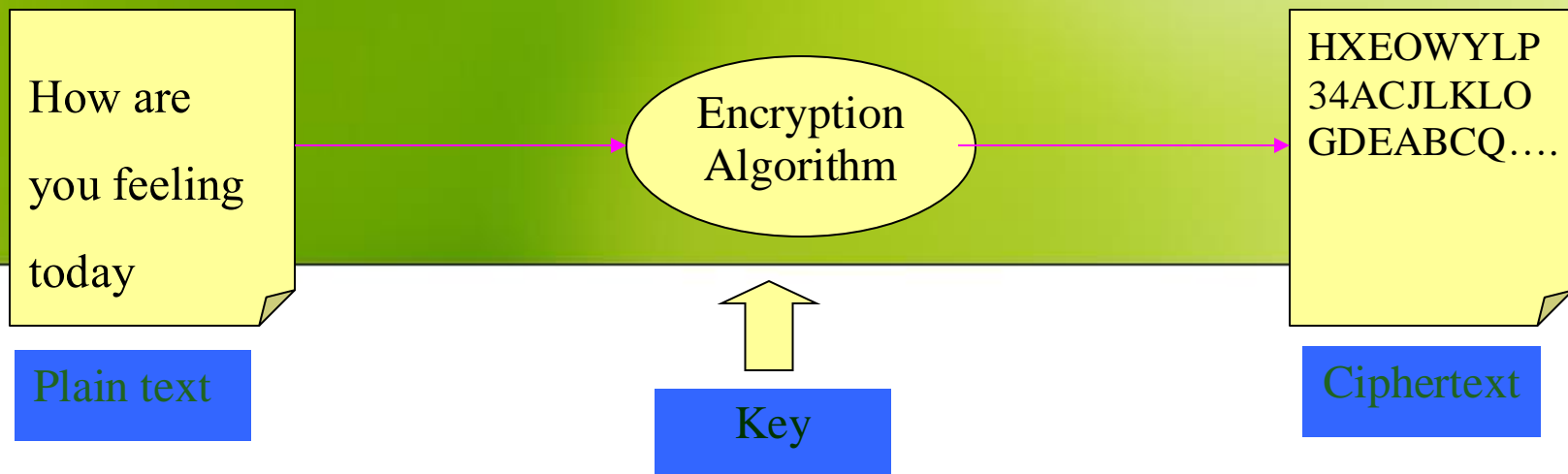
# การเข้ารหัส (Encryption)



แสดงการเข้ารหัส







## ● คริปโตกราฟี (Cryptography)

- **Plain text** คือ ข้อมูลต้นฉบับซึ่งเป็นข้อความที่สามารถอ่านแล้วเข้าใจ
- **Encryption Algorithm** คือ ขั้นตอนวิธีในโปรแกรมคอมพิวเตอร์ที่ใช้ในการแปลงข้อมูลต้นฉบับเป็นข้อมูลที่ได้รับการเข้ารหัส
- **Ciphertext** คือ ข้อมูลหรือข่าวสารที่ได้รับการเข้ารหัส ทำให้อ่านไม่รู้เรื่อง
- **Key** คือ เป็นกุญแจที่ใช้ร่วมกับ อัลกอริทึมในการเข้ารหัส และถอดรหัส

# การเข้ารหัส (Encryption)

มีด้วยกัน 2 ลักษณะ คือ

## 1. การเข้ารหัสแบบสมมาตร (Symmetric Encryption)

วิธีนี้ทั้งผู้รับและผู้ส่งขอความจะทราบคีย์ที่เหมือนกันทั้งสองฝ่ายในการรับหรือส่งข้อความ

## 2. การเข้ารหัสแบบไม่สมมาตร (Asymmetric Encryption)

ใจแนวคิดของการมีคีย์เป็นคู่ ๆ ที่สามารถเข้าและถอดรหัสของกันและกันได้นั้นได้ โดยคีย์แรกจะมีอยู่ที่เฉพาะเจ้าของคีย์ เรียกว่า Private key และคู่ของคีย์ดังกล่าวที่ส่งให้ผู้อื่นใช้ เรียกว่า Public key



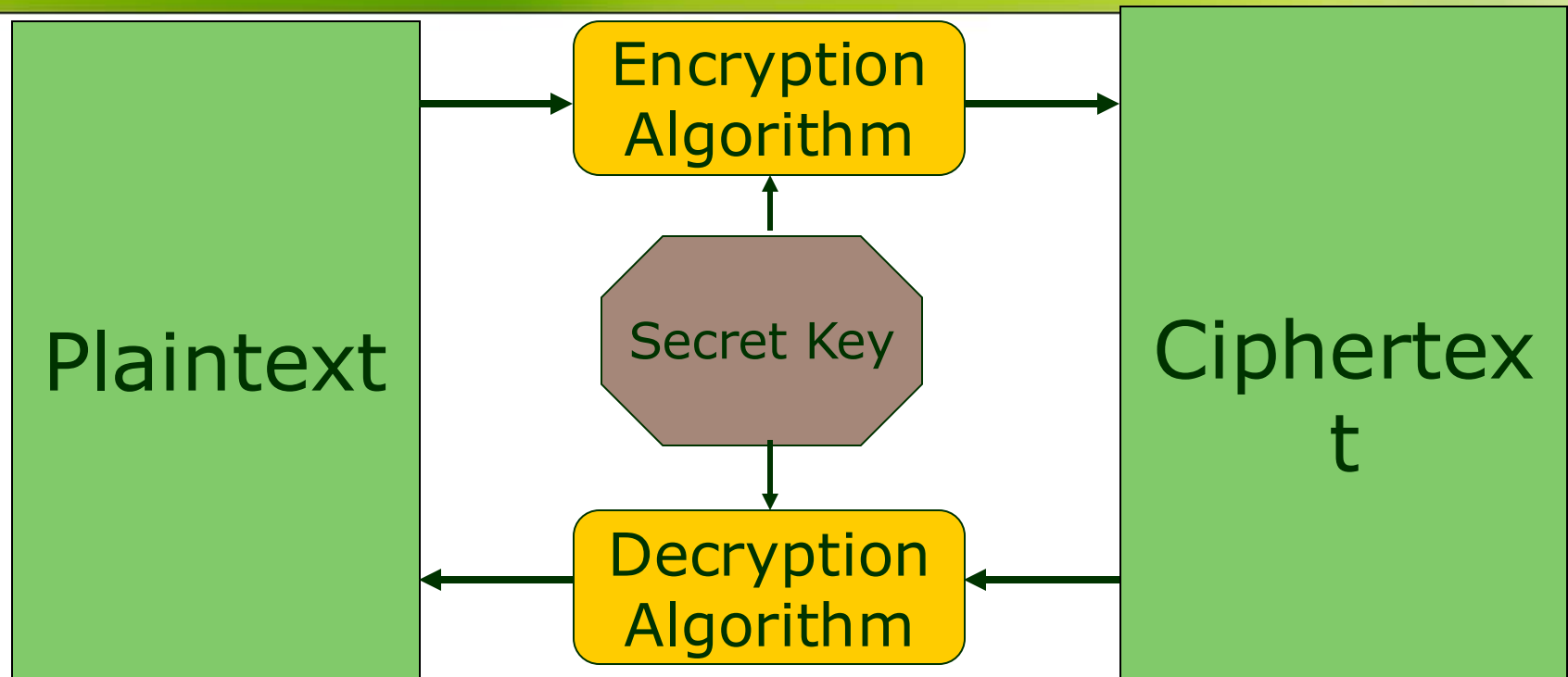
# การเข้ารหัส (Encryption)

## 1. การเข้ารหัสแบบสมมาตร (Symmetric Encryption)

- เป็นการใช้อัลกอริทึม หรือกุญแจในการเข้ารหัสเหมือนกัน ทั้งฝ่ายรับและฝ่ายส่ง
- วิธีนี้ ทั้งผู้รับและผู้ส่งขอความจะทราบคีย์ที่เหมือนกันทั้งสองฝ่ายในการรับหรือส่งขอความ
- ซึ่งหากมีขโมยนำกุญแจดอกนี้ไปได้ ก็สามารถถอดรหัสข้อมูลของเราได้



# การเข้ารหัสแบบสมมาตร (Symmetric Encryption)



แสดงการเข้ารหัสแบบทางเดียวด้วยกุญแจลับ (Secret key encryption)



# การเข้ารหัสแบบสมมาตร

## Symmetric Encryption

การเข้ารหัสแบบสมมาตรนี้ ก่อให้เกิดปัญหา 2 ส่วน คือ

- **ปัญหา Authentication** เนื่องจากผู้อื่นอาจทราบรหัสลับ

ด้วยวิธีใดก็ตามแล้วปลอมตัวเข้ามาส่งข้อความถึงเรา

**ปัญหา Non-repudiation** คือ ไม่มีหลักฐานใดที่พิสูจน์ได้ว่า

ผู้ส่งหรือผู้รับได้กระทำรายการจริง ๆ

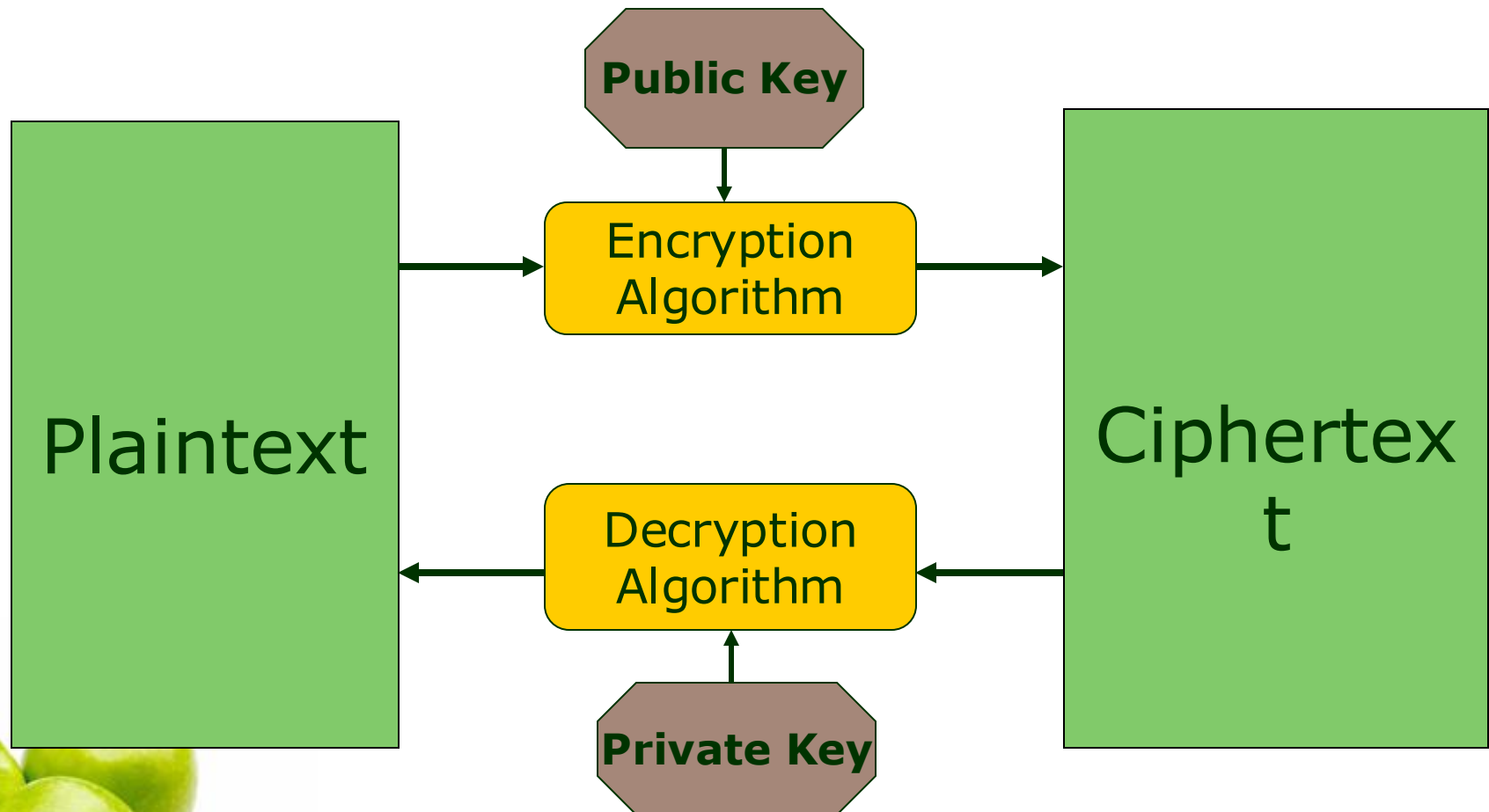


# การเข้ารหัส (Encryption)

## 2. การเข้ารหัสแบบไม่สมมาตร (Asymmetric Encryption)

- แนวคิดของ การมีคีย์เป็นคู่ ๆ ที่สามารถเข้าและถอดรหัสของกันและกันได้นั้นประกอบด้วย กุญแจ 2 ดอก คือ
  - **กุญแจสาธารณะ (Public key)** ใช้สำหรับการเข้ารหัส
  - **กุญแจส่วนตัว (Private key)** ใช้สำหรับการถอดรหัส
- ที่สำคัญกุญแจที่เข้ารหัสจะนำมาถอดรหัสได้ ซึ่ง Public key จะแจกจ่ายไปยังบุคคลต่างๆ ที่ต้องการสื่อสาร ส่วน Private Key จะเก็บไว้ส่วนตัวไม่เผยแพร่ให้ใคร

# การเข้ารหัสแบบไม่สมมาตร (Asymmetric Encryption)



แสดงการเข้ารหัสด้วยกุญแจสาธารณะ (Public key)



# เทคโนโลยีระบบรหัสแบบอสมมาตร (เทคโนโลยี Public Key)



คำว่า **อสมมาตร** แสดงถึงความไม่เหมือนกันสองข้าง ซึ่งในที่นี้  
คือ การใช้กุญแจต่างกัน เรียกว่า**กุญแจคู่** ประกอบด้วย**กุญแจ**  
**ส่วนตัว** (Private Key) และ**กุญแจสาธารณะ** (Public Key) ใน  
ข้างผู้ส่ง และข้างผู้รับ

กุญแจเป็นข้อมูลในรูปอิเล็กทรอนิกส์  
ซึ่งใช้ในการเข้ารหัสและถอดรหัส

ตัวอย่าง

00:bc:73:d4:ce:01:1b:b9:0c:00:15:c7:56



# เทคโนโลยี Public Key

- กุญแจส่วนตัวต้องอยู่กับผู้เป็นเจ้าของเพียงคนเดียว และผู้เป็นเจ้าของต้องไม่ให้ผู้อื่นล่วงรู้ถึงกุญแจส่วนตัวนี้
- กุญแจสาธารณะควรจะอยู่ในที่ซึ่งบุคคลทั่วไปค้นหาได้ โดยสะดวกและไม่จำเป็นต้องเก็บเป็นความลับแต่อย่างใด



# ระบบรหัสแบบอสมมาตร (เทคโนโลยี Public Key)

การรักษาความลับ  
(Confidentiality)

การเข้ารหัส  
(Encryption)

ลายมือชื่อดิจิทัล  
(Digital Signature)

การระบุตัวบุคคล  
(Authentication)

ความแท้จริง  
(Integrity)

การห้ามปฏิเสธ  
ความรับผิดชอบ  
(Non-repudiation)



# การเข้ารหัสแบบไม่สมมาตร (Asymmetric Encryption)

ประโยชน์ของระบบการเข้ารหัสแบบไม่สมมาตร มีดังนี้

1. ให้ความลับของข้อมูลที่จะจัดส่งไป
2. แก้ปัญหาการ Authenticate คือ ตรวจสอบว่าบุคคลที่ส่งข้อมูลเข้ามาเป็นผู้ส่งเองจริง ๆ ซึ่งทำได้โดยใช้วิธีการเข้ารหัสด้วยคีย์ส่วนตัว

\*\* การใช้คีย์ส่วนตัวเข้ารหัสข้อมูลเปรียบได้กับการเซ็นชื่อของเราบนเอกสารที่เป็นกระดาษเพื่อรับรองว่าข้อมูลนี้เราเป็นผู้ส่งจริง

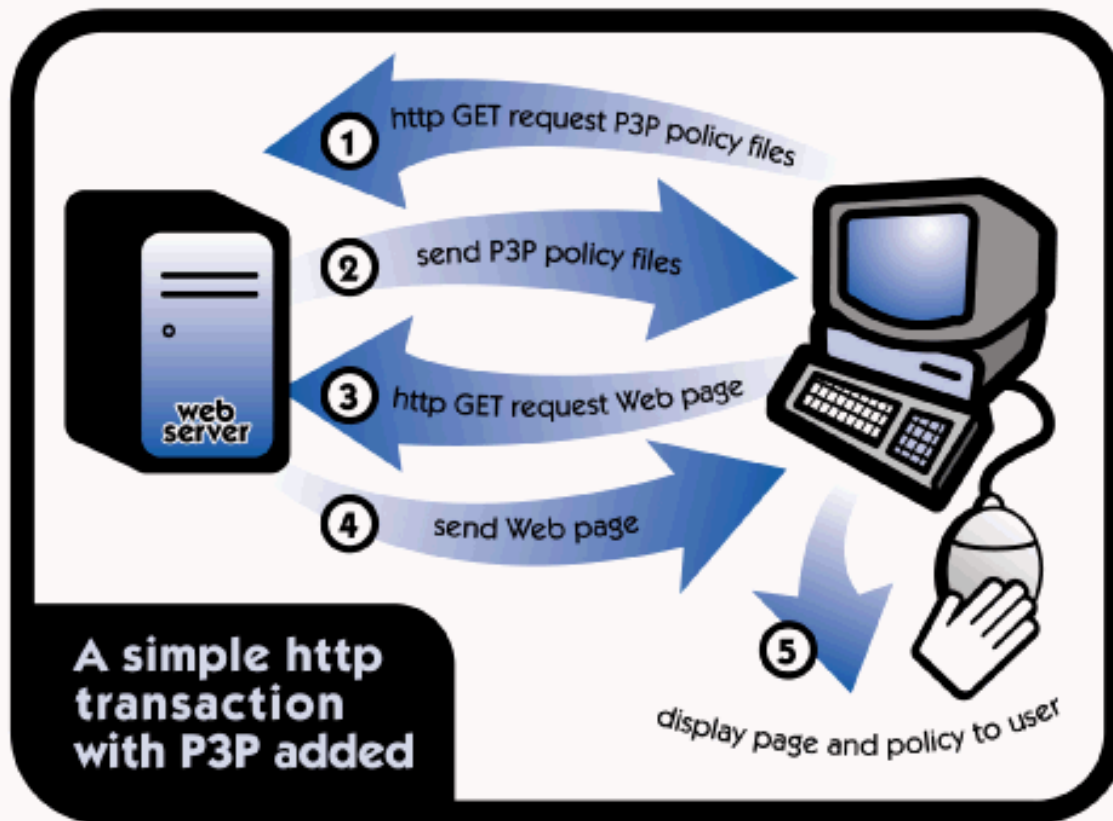


# Platform for Privacy Preference (P3P)

- Platform for Privacy Preference (P3P) เป็นมาตรฐานในการสื่อสารนโยบายความเป็นส่วนตัวส่วนตัวของเว็บไซต์อิเล็กทรอนิกส์กับผู้เยี่ยมชม
- การทำงานมาตรฐานของ P3P เริ่มต้นเมื่อ User ร้องขอเว็บเพจไปยังเว็บไซต์ที่ต้องการ Server ของเว็บไซต์ดังกล่าวจะส่งเว็บเพจกลับไปยัง User ตามที่ร้องขอพร้อมกับแนบไฟล์ประกาศนโยบายความเป็นส่วนตัวส่วนตัวของเว็บไซต์ หากเว็บไซต์ที่ User ร้องขอไม่ได้จัดทำนโยบายความเป็นส่วนตัวส่วนตัวตามมาตรฐานของ P3P Web Server ก็จะไม่ส่งข้อมูลดังกล่าวไปให้ User จะส่งเพียงหน้าเว็บเพจที่ต้องการเท่านั้น จากนั้นโปรแกรม web browser ที่ User ใช้ จะเปรียบเทียบนโยบายความเป็นส่วนตัวส่วนตัวของเว็บไซต์กับของ User ที่กำหนดไว้ หากมีระดับไม่ตรงกัน Web browser จะแจ้งเตือน User ให้พิจารณาว่าจะเยี่ยมชมเว็บไซต์ต่อไปหรือไม่ หรือระงับการทำงานของ Cookies จากเว็บไซต์นั้นไปทันที ซึ่งอาจทำให้ User ไม่สามารถเยี่ยมชมเว็บไซต์นั้นได้ แต่ User จะมีความปลอดภัยจากการนำข้อมูลส่วนบุคคลไปใช้ที่อื่นได้



# Platform for Privacy Preference (P3P)



แสดงการทำงานของมาตรฐาน P3P เพื่อป้องกันสิทธิส่วนบุคคล  
ของผู้เยี่ยมชมเว็บไซต์

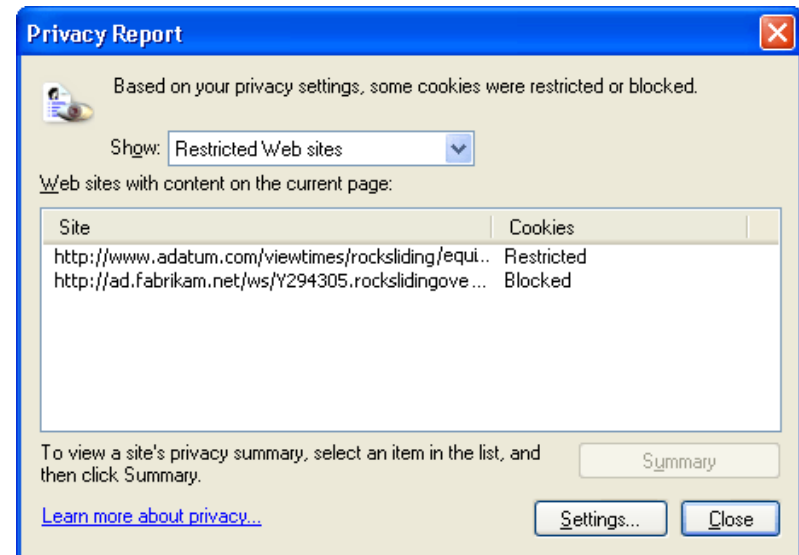
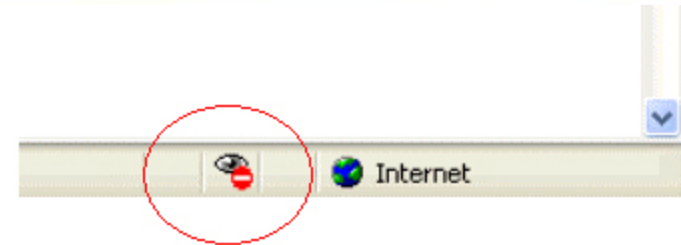
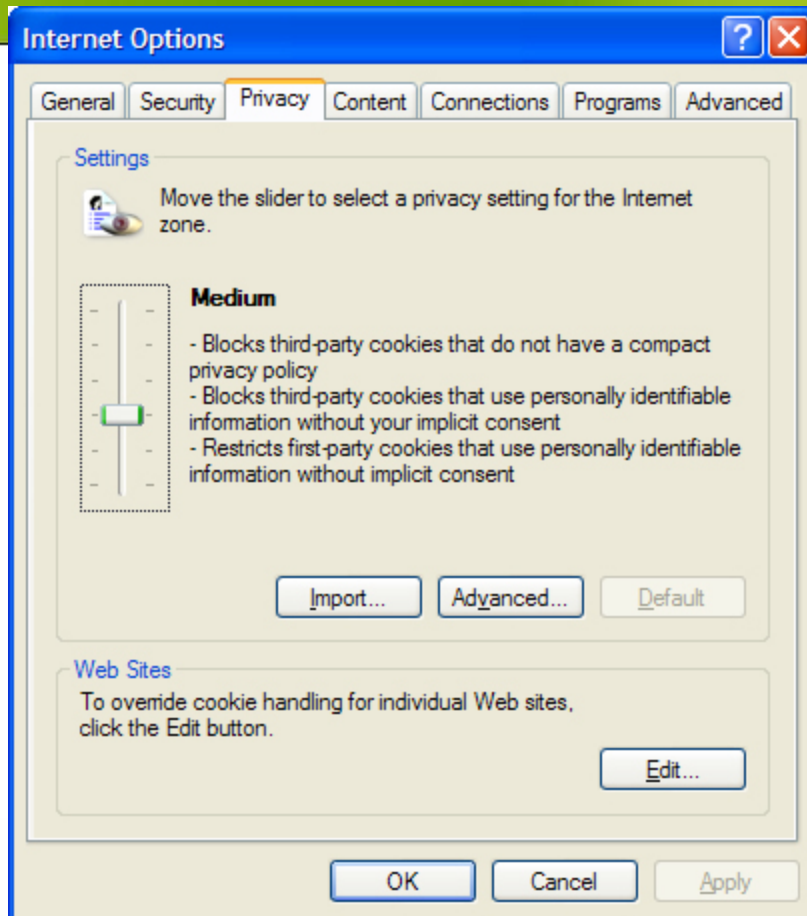
# Platform for Privacy Preference (P3P)

- ปัจจุบันโปรแกรม Web browser ที่ใช้กันทั่วไป เช่น Internet Explorer, Mozilla Firefox สามารถรองรับมาตรฐาน P3P โดยอนุญาตให้ผู้ใช้งานกำหนดระดับการยอมรับไฟล์ Cookies ได้ เช่น Medium level จะระงับ Cookies ของเว็บไซต์ที่มีนโยบายความเป็นส่วนตัวไม่รัดกุม คือ ไม่มีการแยกข้อมูลที่เป็นส่วนตัวออก





# Platform for Privacy Preference (P3P)



แสดงการตั้งระดับการยอมรับไฟล์ Cookies ของเว็บไซต์

# การเข้ารหัส (Encryption)

การรักษาความปลอดภัยของข้อมูลที่ส่งผ่านเครือข่ายอินเทอร์เน็ตที่นิยมใช้งานมากที่สุดคือ “การเข้ารหัส (Encryption)” โดยเว็บไซต์ที่ใช้วิธีการเข้ารหัสเพื่อป้องกันข้อมูลจะใช้ Digital Certification ร่วมกับ Security Protocol เพื่อทำให้มีความปลอดภัยสูงขึ้น โดยโปรโตคอลที่นิยมใช้งานมี 3 ชนิด คือ

- Secure Socket Layer (SSL)
- Secure Hypertext Transport Protocol S-HTTP
- Secure Electronic Transaction (SET)



# SSL (Secure Socket Layer)



เป็นโปรโตคอลที่พัฒนาโดย Netscape ใช้สำหรับตรวจสอบและเข้ารหัสด้วยกุญแจสาธารณะแก่ข้อมูล ก่อนที่ข้อมูลจะถูกส่งออกไปบนเครือข่ายอินเทอร์เน็ต โดยจะนำข้อมูลมาเข้ารหัสและถอดรหัสด้วยเทคนิค Cryptography และใบรับรองอิเล็กทรอนิกส์(Digital Certificates) และมีการทำงานที่ TCP/IP จะใช้ SSL ในการทำระบบรักษาความปลอดภัย

ส่วนการใช้งานในเว็บไซต์ เมื่อผู้ใช้งานต้องการติดต่อมายัง Server ผู้ใช้จะต้องทำการเรียก Web Browser โดยในช่อง URL จะมีโปรโตคอลเป็น <https://> แทน <http://> เป็นตัวบอกว่าต้องการใช้ SSL ในการติดต่อ Server

# SSL (Secure Socket Layer)

เราจะทราบได้อย่างไรว่าเว็บไซต์ที่เราเข้าไปเยี่ยมชมนั้นเป็นระบบ SSL หรือไม่ก็คงต้องสังเกตจาก Icon Security หรือ URL ที่แสดงผลอยู่บนเว็บเบราว์เซอร์



โดยกลไกการรักษาความปลอดภัย มีดังนี้

- 1) ความปลอดภัยของข้อความ (Message Privacy)
- 2) ความสมบูรณ์ของข้อความ (Message Integrity)
- 3) ความน่าเชื่อถือ (Mutual Authentication)
- 4) ใบรับรองดิจิทัล (Digital Certificate)



# Secure Hypertext Transport Protocol

## S-HTTP

ส่วนของโปรโตคอล HTTP ทำหน้าที่ตรวจสอบสิทธิ์ผู้ใช้  
ซึ่งจะเข้ารหัสการลงลายเซ็นดิจิทัล (Digital Signature)  
ระบบนี้จะอนุญาตให้ผู้ใช้และเครื่องให้บริการติดต่อกันได้  
เมื่อทั้ง 2 ฝ่ายมี Digital Certificate  
ระบบรักษาความปลอดภัยรูปแบบนี้ยุ่งยากกว่า SSL แต่  
มีความปลอดภัยมากกว่า **นิยมใช้ในธุรกิจการเงิน**



# ระบบ Secure Electronic Transaction (SET)

**ระบบ SET หรือ Secure Electronic Transaction** เป็นระบบเพื่อใช้สำหรับตรวจสอบการชำระเงินด้วยบัตรเครดิตอย่างปลอดภัยบนอินเทอร์เน็ต ซึ่งได้รับการสนับสนุนเริ่มต้นโดย MasterCard, Visa, Microsoft, Netscape และอื่น ๆ โดยการสร้างรหัส SET ซึ่งเป็นการเข้ารหัสด้วยกุญแจสาธารณะ



# ระบบ Secure Electronic Transaction (SET)

ระบบ SET นี้ถูกออกแบบมาเพื่อใช้กับกิจกรรมการทำพาณิชย์อิเล็กทรอนิกส์ โดยระบบนี้สามารถรักษาความลับของข้อมูลข่าวสารที่ถูกส่งผ่านระบบเครือข่ายคอมพิวเตอร์ได้เป็นอย่างดี และรับประกันความถูกต้องโดยไม่มีการปลอมแปลงของข้อมูลที่เกี่ยวข้องกับการเบิกจ่ายเงินได้เป็นอย่างดีด้วย

นอกจากนี้ยังสามารถที่จะบ่งชี้ชัดได้ว่าใครเป็นผู้ซื้อและผู้ค้าได้อย่างถูกต้องโดยไม่มีการปลอมแปลง





# เปรียบเทียบ SET กับ SSL

## ระบบ SET

### ข้อดี

1. ใช้วิธีการเข้ารหัสลับที่ดีกว่าจึงให้ความปลอดภัยสูงกว่า
2. ร้านค้าสามารถพิสูจน์ทราบลูกค้าได้ทันทีว่าเป็นผู้ได้รับอนุญาตในระบบหรือไม่และมีเครดิตเพียงพอในการซื้อหรือไม่
3. สามารถเปิดเผยความลับหรือข้อมูลการทำธุรกิจของลูกค้าจากร้านค้าและจากธนาคารผู้ออกบัตรได้

### ข้อเสีย

1. ยังไม่มีการทดสอบและทดลองใช้อย่างเพียงพอ
2. ยังไม่มีการนำไปใช้เชิงธุรกิจในวงกว้างมากนัก



# เปรียบเทียบ SET กับ SSL

## ระบบ SSL

### ข้อดี

1. **ลงทุนน้อย** หรือแทบไม่มีเลย เพราะปัจจุบันใช้ใบในวงกว้าง
2. สามารถควบคุมการเข้าถึงข้อมูลส่วนต่าง ๆ ภายในระบบของผู้ใช้ได้ หลังจากที่ถูกผู้ใช้ได้รับอนุญาตให้เข้ามาในระบบ
3. สามารถ**ใช้ข้อมูลร่วมกัน**ได้ระหว่างสองจุด
4. มีระบบ**ป้องกันและตรวจสอบ**ความถูกต้องของข้อมูลได้

### ข้อเสีย

1. ใช้วิธีการเข้ารหัสที่สลับซับซ้อน ความปลอดภัยไม่เพียงพอ
2. ทำการสื่อสารอย่างปลอดภัยได้เพียงสองจุด แต่ระบบพาณิชย์อิเล็กทรอนิกส์ที่ใช้บัตรต้องใช้มากกว่าสองจุดในเวลาเดียวกัน
3. มีความเสี่ยงสูงเนื่องจากไม่มีการรับรองทางอิเล็กทรอนิกส์ระหว่างทุกฝ่ายที่ทำการซื้อขายในขณะนั้น และความเสี่ยงในการรั่วไหลของข้อมูลลูกค้า

# ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature)

- สำหรับในการทำธุรกรรมทางอิเล็กทรอนิกส์นั้นจะใช้ **ลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signature)** ซึ่งมีรูปแบบต่างๆ เช่น สิ่ง  
ที่ระบุตัวบุคคลทางชีวภาพ (ลายพิมพ์นิ้วมือ เสียงปรานตา เป็นต้น)  
หรือ จะเป็นสิ่งที่มอบให้แก่บุคคลนั้นๆ ในรูปแบบของ รหัส  
ประจำตัว ตัวอย่างที่สำคัญของลายมือชื่ออิเล็กทรอนิกส์ ที่ได้รับการยอมรับกันมากที่สุดอันหนึ่ง คือ **ลายมือชื่อดิจิตอล (Digital Signature)** ซึ่งจะเป็นองค์ประกอบหนึ่งใน โครงสร้างพื้นฐานกุญแจ  
สาธารณะ (Public Key Infrastructure, PKI)



# Digital Signature คืออะไร

- **ลายเซ็นดิจิทัล (Digital Signature)** เป็นสิ่งที่แสดงยืนยันตัวตนบุคคล เป็นข้อมูลที่แนบไปกับข้อความที่ส่งไป เพื่อเป็นการแสดงตัวตน (Authentication) ว่าผู้ส่งข้อความเป็นใคร โดยข้อมูลนั้นได้ถูกส่งมาจากผู้ส่งคนนั้นจริงๆ และข้อความไม่ได้ถูกเปลี่ยนแปลงและแก้ไข
- ใช้กับการพิสูจน์ความถูกต้องของเอกสารตามกฎหมาย เช่น ด้านการเงิน การทำสัญญา และเอกสารอื่นๆ ว่าเป็นของแท้ นั้น สามารถทำได้โดยการตรวจสอบความถูกต้องของลายเซ็นของผู้มีอำนาจอนุมัติ



# ลายเซ็นดิจิทัล (Digital Signature)

การเข้ารหัสข้อความที่ยาวนั้น ค่อนข้างเสียเวลา เนื่องจากขั้นตอนการเข้ารหัสต้องใช้การคำนวณเป็นอย่างมาก **จึงมีการสร้างขั้นตอนที่คำนวณได้อย่างรวดเร็ว โดยเปลี่ยนข้อความทั้งหมดให้เหลือเพียงข้อความสั้น ๆ เรียกว่า “Message digest”** ซึ่งจะถูกสร้างขึ้นด้วยกระบวนการเข้ารหัสชนิดนิยมที่เรียกว่า One-way hash function

จะใช้ message digest นี้ในการเข้ารหัสเพื่อเป็นลายเซ็นดิจิทัล (Digital Signature) โดยจะแจก Public key ไปยังผู้ที่ต้องการติดต่อ



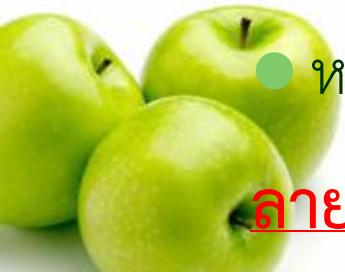
# ลายเซ็นดิจิทัล (Digital Signature)

- ประโยชน์ของลายเซ็นดิจิทัล (Digital signature) มีดังนี้
  1. ยากแก่การปลอมแปลงลายเซ็น
  2. ข้อความในเอกสารไม่ถูกลักลอบอ่านและแก้ไข
  3. ระยะเวลาไม่เป็นอุปสรรคในการตรวจสอบความถูกต้อง
  4. สำเนาของเอกสารมีสถานะเทียบเท่ากับเอกสารต้นฉบับ
  5. มีบุคคลที่สาม (Certifies) หรือองค์กรกลาง [Certification Authority (CA)] เป็นผู้รับรองความถูกต้องของลายเซ็น (Certificate)



# ใบรับรองอิเล็กทรอนิกส์ – Digital Certification

- รายละเอียดในใบรับรองอิเล็กทรอนิกส์มีดังนี้คือ
  - ข้อมูลระบุผู้ที่ได้รับการรับรอง ได้แก่ ชื่อ องค์กร ที่อยู่
  - ข้อมูลผู้ออกใบรับรอง ได้แก่ ลายมือชื่อดิจิทัลขององค์กรที่ออกใบรับรอง
  - กุญแจสาธารณะของผู้ที่ได้รับการรับรอง
  - วันหมดอายุของใบรับรองอิเล็กทรอนิกส์
  - ระดับชั้นของใบรับรองอิเล็กทรอนิกส์ มี 4 ระดับ ในระดับ 4 จะมีการตรวจสอบเข้มงวดที่สุด
  - หมายเลขประจำตัวของใบรับรองอิเล็กทรอนิกส์ หรือเรียกว่า ลายมือชื่อดิจิทัลของผู้ประกอบการรับรอง





# ใบรับรองอิเล็กทรอนิกส์ – Digital Certification

- ประเภทของใบรับรองอิเล็กทรอนิกส์
  - ใบรับรองอิเล็กทรอนิกส์สำหรับบุคคล เป็นใบรับรองที่ใช้ในการยืนยันตัวบุคคลบนโลกอิเล็กทรอนิกส์
  - ใบรับรองอิเล็กทรอนิกส์สำหรับเครื่องให้บริการเว็บ หรือที่เรียกว่าเว็บเซิร์ฟเวอร์ ใช้สำหรับเป็นช่องทางการสื่อสารแบบปลอดภัยระหว่างเครื่องบริการบนเว็บ สามารถประยุกต์ใช้งานรักษาความลับของข้อมูลที่รับส่งผ่านทางเครือข่ายอินเทอร์เน็ต เช่น รหัสผ่าน หมายเลขเครดิต



# ใบรับรองอิเล็กทรอนิกส์ - Certification Authority (CA)

- ผู้ให้บริการออกใบรับรอง Certification Authority (CA)
- CA หรือ Certificate Authority คือผู้ประกอบกิจการ ออกใบรับรองอิเล็กทรอนิกส์ และเป็นที่ยอมรับ ซึ่งเปรียบเสมือนบัตรประจำตัวที่ใช้ในการระบุตัวบุคคล
- บทบาทหน้าที่หลักคือ
  - ให้บริการเทคโนโลยีการเข้ารหัสโดยอาศัยเทคโนโลยีที่เรียกว่า เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure - PKI)
  - การให้บริการออกใบรับรอง
  - บริการเสริมอื่นๆ ได้แก่ การตรวจสอบสัญญาต่างๆ การประกัน



# ทำไมต้องใช้ใบรับรองอิเล็กทรอนิกส์

## Certification Authority (CA)

- การใช้ใบรับรองอิเล็กทรอนิกส์ ผู้ใช้จะสามารถมั่นใจได้ว่า
  - ข้อมูลต่างๆ ที่ได้รับมีความถูกต้อง ครบถ้วน ไม่ถูกเปลี่ยนแปลงแก้ไข
  - สามารถพิสูจน์ และยืนยันตัวบุคคลได้ว่าเป็นบุคคลผู้ที่เราติดต่อด้วยจริง
  - สามารถรักษาความลับของข้อมูลได้ หากเป็นข้อมูลที่ต้องการให้ผู้รับเท่านั้นที่สามารถอ่านอีเมลฉบับนั้นๆได้ ซึ่งกรณีนี้จะต้องมีการใช้ใบรับรองอิเล็กทรอนิกส์ในการเข้ารหัสก่อนทำการส่งอีเมลไปยังผู้รับ



# ทำไมต้องใช้ใบรับรองอิเล็กทรอนิกส์

## Certification Authority (CA)

- ใบรับรองอิเล็กทรอนิกส์สามารถทำอะไรได้บ้าง  
ใบรับรองอิเล็กทรอนิกส์นั้นสามารถนำไปประยุกต์ใช้ได้ 2 ลักษณะดังนี้

1. การเข้ารหัส (Encryption)

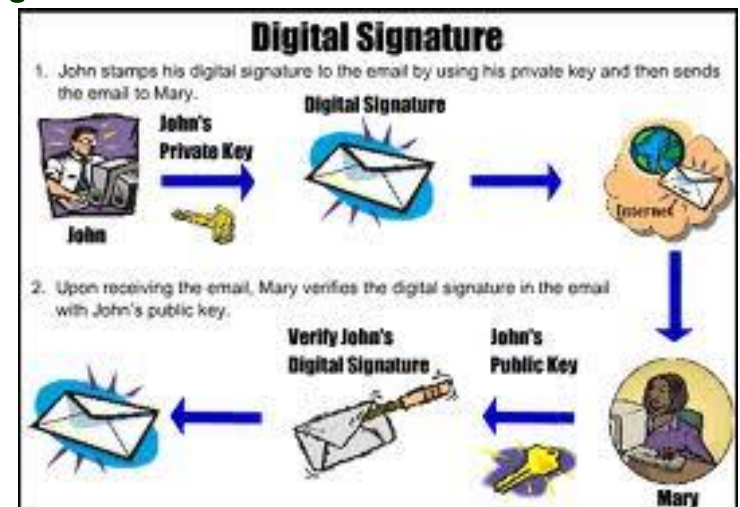


2. การลงลายมือชื่อดิจิทัล (Digital Signature)



# เทคโนโลยีสำหรับระบบรักษาความปลอดภัย

- เพื่อป้องกันเครือข่ายขององค์กรให้พ้นจากบุคคลผู้ไม่ประสงค์ดี
- ระบบรักษาความปลอดภัย แบ่งเป็น 2 ด้าน คือ
  - การรักษาความปลอดภัยให้กับเครือข่ายองค์กร
  - การรักษาความปลอดภัยในการส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ต



ตัวอย่างองค์กรที่ใช้ CA

<http://www.ca.tot.co.th/faq.php>

ทดลองสมัครและติดตั้งใบรับรองอิเล็กทรอนิกส์สำหรับบุคคล

<http://gca.thaigov.net/>



Thank  
you.

