เชิญชวนนำเข้า RMUTI Root Certificate Authority ในเครื่องคอมพิวเตอร์

Author : Prakai Nadee

สำนักวิทยบริการและเทคโนโลยีสารสนเทศขอเชิญชวนอาจารย์ เจ้าหน้าที่ และนักศึกษาติดตั้ง RMUTI Root Certificate Authority (RMUTI CA) ในเครื่องคอมพิวเตอร์และอุปกรณ์พกพา
เพื่อใช้สำหรับเข้ารหัสการสื่อสารกับบริการอิเล็กทรอกนิกส์ของมหาวิทยาลัยอย่างปลอดภัย

การเข้ารหัสข้อมูล

ในกระบวนการสื่อสารของคอมพิวเตอร์หรืออินเทอร์เน็ต
หากต้องการให้คู่การสื่อสารนั้นปลอดภัยจากการดักฟังข้อมูลของบุคคลที่ไม่หวังดี
ข้อมูลที่สื่อสารระหว่างคู่การสื่อสารนั้นจะต้องผ่านการเข้ารหัส ข้อมูลที่ไม่ผ่านการเข้ารหัสเมื่อถูกดักฟัง
จะสามารถเห็นและเข้าใจในข้อมูลนั้นได้ง่าย ส่วนข้อมูลที่ผ่านการเข้ารหัสแล้ว แม้จะถูกดักฟัง
ข้อมูลที่ได้ไปนั้นจะมีรูปแบบที่ทำความเข้าใจได้ยาก โดยจะไม่สามารถถอดรหัสไปเป็นข้อมูลต้นฉบับได้
หรืออาจต้องเสียเวลาในการถอดรหัสเป็นเวลานานในกรณีของการเลือกวิธีการเข้ารหัสที่ไม่แข็งแรงพอ

ตัวอย่างของการสื่อสารที่สมควรผ่านการเข้ารหัส เช่น การใช้บริการบนเว็บไซต์ที่ต้องยืนยันตัวตน หรือการล็อกอิน
เครื่องผู้ใช้จะส่งชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ไปยังเว็บเซิร์ฟเวอร์ หากข้อมูลไม่มีการเข้ารหัส
บุคคลที่ดักฟังข้อมูลจะสามารถดักฟังและเห็นชื่อผู้ใช้กับรหัสผ่านที่แท้จริงได้ทันที

```
[Browser]--myname/mypass---+------------->[Server]
      |                              v                          {hacker}
```

แต่หากมีการเข้ารหัสข้อมูล ผู้ที่ดักฟังจะมองเห็นข้อมูลที่ไม่เหมือนเดิม ซึ่งไม่สามารถทำให้เป็นข้อมูลแท้จริงได้
หรือใช้เวลานานในการดำเนินการให้ได้ข้อมูลแท้จริง

```
[Browser/encrypt]--x$y%a#n/0+a@c!h--+---->[Server/decrypt]
                          |                                     v
                            {hacker}
```

การเข้ารหัสข้อมูลทางคอมพิวเตอร์จำเป็นต้องใช้ใบรับรองทางดิจิตอล (Digital Certificate) ขออธิบายโดยย่อดังนี้
องค์ประกอบของการเข้ารหัสจะต้องใช้ใบรับรองมี 3 ส่วนคือ

1. ใบรับรองของผู้ให้การรับรอง (Certificate Authority)
2. ใบรับรองของแม่ข่าย (Server Certificate)
3. ใบรับรองของลูกข่ายหรือผู้ใช้ (Client/User Certificate)

Certificate Authority

ส่วนประกอบของการเข้ารหัสส่วนหลักคือ ใบรับรองของผู้ให้การรับรอง [wikipedia]
เป็นใบรับรองของคนกลางที่ใช้ในการรับรองหรือสร้างความน่าเชื่อถือของการสื่อสารระหว่างแม่ข่ายกับลูกข่ายหรือผู้ใช้
ใบรับรองนี้จะต้องติดตั้งทึ้งบนเครื่องแม่ข่ายและเครื่องลูกข่าย

ผู้ให้บริการออกใบรับรองที่สามารถใช้บริการได้มีมากมาย เช่น Versign, Thawte, GeoTrus เป็นต้น
โดยการขอใบรับรองจะต้องชำระค่าออกใบรับรอง มีระยะเวลาการใช้งานหรืออายุของใบรับรองที่จำกัดเป็นปี
ใบรับรองของผู้ให้บริการเหล่านี้จะได้รับการติดตั้งเครื่องของผู้ใช้อยู่แล้ว โดยติดตั้งมากับระบบปฏิบัติการของเครื่อง
ผู้ใช้จึงไม่ต้องดำเนินการใดๆ กับเครื่องของตน

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้ดำเนินการสร้าง Certificate Authority ขึ้นมาและรับรองตนเอง
(Self-signed Certificate) เพื่อใช้ภายในมหาวิทยาลัย เรียกใบรับรองนี้ว่า Root Certificate Authority
(ดาวน์โหลดได้ที่ http://ca.rmuti.ac.th/ca.certs/RMUTi-CA.crt) เนื่องจากเป็นใบรับรองที่สร้างขึ้นเอง
ผู้ใช้จึงจำเป็นต้องดำเนินการนำเข้าใบรับรองไปในเครื่องด้วยตนเอง

Server Certificate

ใบรับรองแม่ข่าย [wikipedia] เป็นส่วนประกอบการเข้ารหัสที่ใช้แสดงความน่าเชื่อถือของแม่ข่ายที่มีต่อเครื่องลูกข่าย
หรือทำให้เครื่องลูกข่ายเชื่อถือในความเป็นตัวตนของเครื่องแม่ข่าย
ผู้ติดตั้งเครื่องแม่ข่ายจะต้องขอใบรับรองของเครื่องแม่ข่ายจากผู้ออกใบรับรอง และนำใบรับรองที่ได้รับมาติดตั้งในเครื่องแม่ข่าย

หลายๆ บริการ โดยเฉพาะการบริการแบบ Server/Client เช่น บริการเว็บ จะใช้ใบรับรองเพียง 2
ส่วนคือ ใบรับรองของผู้ให้การรับรอง และใบรับรองของเครื่องแม่ข่าย แต่ต้องติดตั้งทั้งในเครื่องแม่ข่ายและเครื่องลูกข่าย

- เครื่องแม่ข่าย: ติดตั้งใบรับรองของผู้ให้การรับรองและใบรับรองของเครื่องแม่ข่าย
- เครื่องลูกข่าย: ติดตั้งใบรับรองของผู้ให้การรับรอง

```
+---------------[Certificate Authority]--------------+        |
                                                       |
```

```
   Root CA                                                  Root CA, Server CA
    |                                                              |        v
                                                   v



[Client/User] ---------------------- [Server]
```

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
ได้ดำเนินการออกใบรับรองและติดตั้งให้แก่เครื่องแม่ข่ายในมหาวิทยาลัยบางส่วนแล้ว เช่น เว็บเซิร์ฟเวอร์หลัก (https://www.rmuti.ac.th) ระบบเครือข่ายคอมพิวเตอร์แบบไร้สาย (RMUTI-WiFi) เป็นต้น

Client/User Certificate

เป็นใบรับรองที่ใช้สร้างความน่าเชื่อถือให้เครื่องลูกข่ายที่มีต่อเครื่องแม่ข่าย หรือสร้างความน่าเชื่อถือระหว่างผู้ใช้ เช่น การใช้ยืนยันความน่าเชื่อถือของอีเมล์ที่ผู้ใช้ส่งถึงกัน ป้องกันการปลอมแปลงอีเมล์ระหว่างผู้ใช้ โดยผู้ใช้ทั้งสองฝ่ายจะต้องขอใบรับรองไปประกอบการเข้ารหัสหรือคำนวนเอกลักษณ์เฉพาะของเนื้อหาในเมล์ก่อนส่งเมล์ไปยังผู้ใช้อีกคน

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ อยู่ระหว่างการพัฒนาเครื่องมือเพื่อเปิดโอกาสให้อาจารย์ เจ้าหน้าที่และนักศึกษาของมหาวิทยาลัยลงทะเบียนขอรับใบรับรองได้โดยสะดวก

ระบบของมหาวิทยาลัยที่เปิดให้บริการด้วยการเข้ารหัส

- เว็บไซต์/เว็บเมล์ (https://www.rmuti.ac.th, https://www.rmuti.ac.th/m)
- เครือข่ายคอมพิวเตอร์แบบไร้สาย (RMUTI-WiFi)
- ระบบจัดการข้อมูลและบริการอินเทอร์เน็ต (https://www.rmuti.ac.th/network/services)

คู่มือการนำเข้าใบรับรองดิจิตอล

- การนำเข้าใบรับรองในเครื่องผู้ใช้
  - สำหรับ Windows (XP/Vista/7/2000/2003/2008)
  - สำหรับ Windows 8
  - สำหรับ iOS (iPhone/iPad/iPod)
  - สำหรับ Android
- การขอรับและติดตั้งใบรับรองสำหรับเครื่องแม่ข่าย: ติดต่อฝ่ายเทคโนโลยีสารสนเทศเพื่องานวิชาการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ