ความมั่นใจในการเข้าใช้เว็บไซต์ที่มีการเข้ารหัส

อมรรัตน์ ศรีสุรกานนท์*

อินเทอร์เน็ตเป็นช่องทางการเชื่อมโยงระหว่างระบบเครือข่ายจำนวนมหาศาลทั่วโลกเข้าด้วยกันภายใต้หลักเกณฑ์มาตรฐานเดียวกัน นั่นคือ การใช้โพรโทคอลทีซีพี/ไอพี ในการแลกเปลี่ยนข้อมูลเพื่อการสื่อสารถึงกันได้โดยสะดวก รวดเร็ว โดยระยะเริ่มแรก (พ.ศ.2512) อินเทอร์เน็ตเป็นช่องทางการสื่อสารสำหรับวงการทหารเท่านั้นใช้ชื่อว่า โครงการอาร์พาเน็ต (ARPanet) (สมใจ บุญศิริ 2538 : 1) ต่อมามีการขยายลักษณะการใช้งานที่หลากหลายมากขึ้น ซึ่งปัจจุบันมีการใช้อินเทอร์เน็ตทั้งในกิจกรรมทางด้านการศึกษา ธุรกิจการค้า ความบันเทิง และอื่น ๆ เมื่ออินเทอร์เน็ตได้รับความนิยมมีผู้เข้าใช้บริการกันมาก กลุ่มที่ก่อกวนความสงบสุขในสังคมอินเทอร์เน็ตก็เกิดขึ้นเป็นเงาตามตัว เช่น การส่งไวรัสคอมพิวเตอร์แฝงมาในกิจกรรมต่าง ๆ เพื่อเข้าทำลายข้อมูลในเครื่องคอมพิวเตอร์ของผู้เข้าใช้อินเทอร์เน็ต การละเมิดสิทธิ์ส่วนตัวผู้อื่น การหลอกลวงหรือล่อลวงผู้อื่นผ่านการสนทนาออนไลน์ ซึ่งอาจจะนำไปสู่การเกิดอาชญากรรม การลักลอบขโมยข้อมูลโดยผู้ไม่ประสงค์ดีสร้างเว็บไซต์เลียนแบบให้ผู้ใช้หลงเชื่อและแจ้ง Username และ Password เกิดปัญหาการขโมยโอนเงินจากบัญชีหรือการลักลอบเข้าใช้ระบบ ปลอมแปลงเข้าไปทำธุรกรรมต่าง ๆ แทนผู้อื่น โดยไม่สามารถระบุตัวตนของผู้ใช้ นั้น ๆได้ เหล่านี้เป็นสิ่งที่คุกคามความเป็นอยู่ของผู้คนในสังคม ทำให้เกิดพระราชบัญญัติ ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 ขึ้น

การเข้ารหัสกับความปลอดภัยบนเครือข่ายอินเทอร์เน็ต

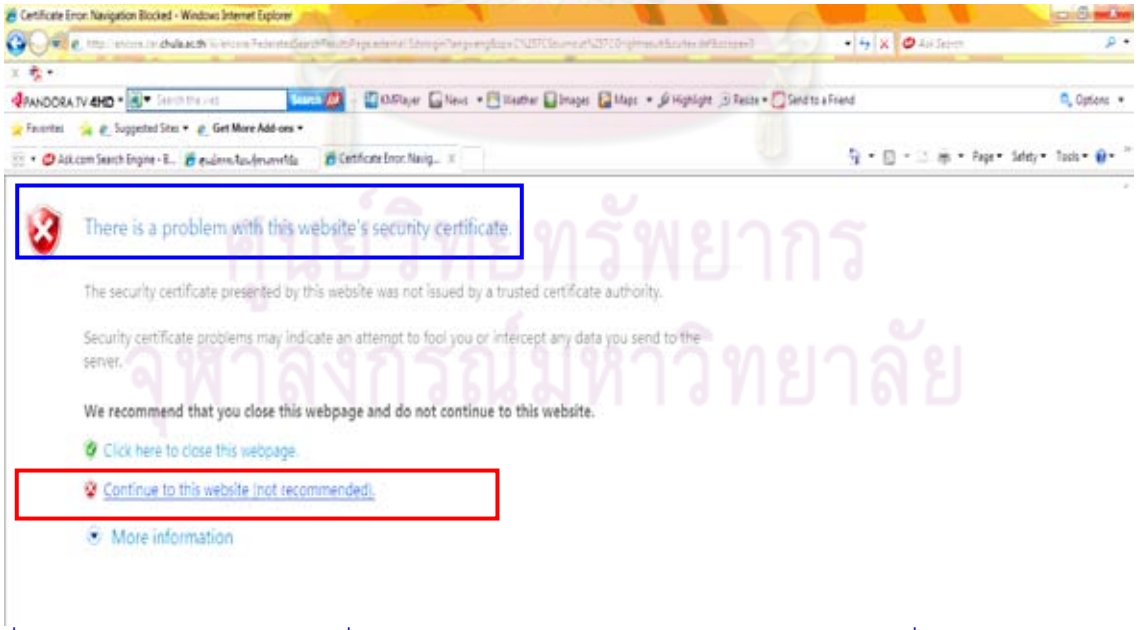
การมีพระราชบัญญัติ ว่าด้วย การกระทำผิดทางคอมพิวเตอร์พ.ศ. 2550 เป็นผลให้ผู้ให้บริการเครือข่ายอินเทอร์เน็ตต้องจัดเก็บข้อมูลการเข้าใช้เครือข่ายของผู้เข้าใช้บริการเครือข่าย เพื่อยืนยันว่ามีการใช้เครือข่ายในช่วงเวลาใด โดยใครบ้าง โดยผู้ให้บริการจะจัดให้มีหน้าเว็บไซต์ไว้ให้ผู้เข้าใช้บริการเครือข่ายต้องพิมพ์ Username และ Password ในการแสดงตนก่อนการเข้าใช้เครือข่าย และเพื่อป้องกันมิให้ผู้ไม่หวังดีดักขโมยข้อมูลหน้าเว็บไซต์นั้น ซึ่งมักจะเป็นเว็บไซต์ที่มีการเข้ารหัส

โดยปกติผู้ใช้อินเทอร์เน็ตจะคุ้นเคยกับการใช้ http:// ซึ่งเป็นโพรโทคอล (Protocol) มาตรฐานของการเข้าไปใช้ดูข้อมูลจากเว็บไซต์ ต่าง ๆ การใช้วิธีการนี้อาจเป็นช่องทางที่เปิดโอกาสให้ผู้ไม่หวังดีมาลักลอบขโมยข้อมูล ในขณะที่มีการส่งข้อมูลระหว่างผู้ใช้บริการและเครื่องแม่ข่ายของผู้ให้บริการบนระบบเครือข่ายอินเทอร์เน็ตได้โดยง่าย เพราะไม่มีการเข้ารหัสใด ๆ เช่น ผู้ใช้อินเทอร์เน็ตพิมพ์อักษร A ผู้ลักลอบดักขโมยข้อมูล

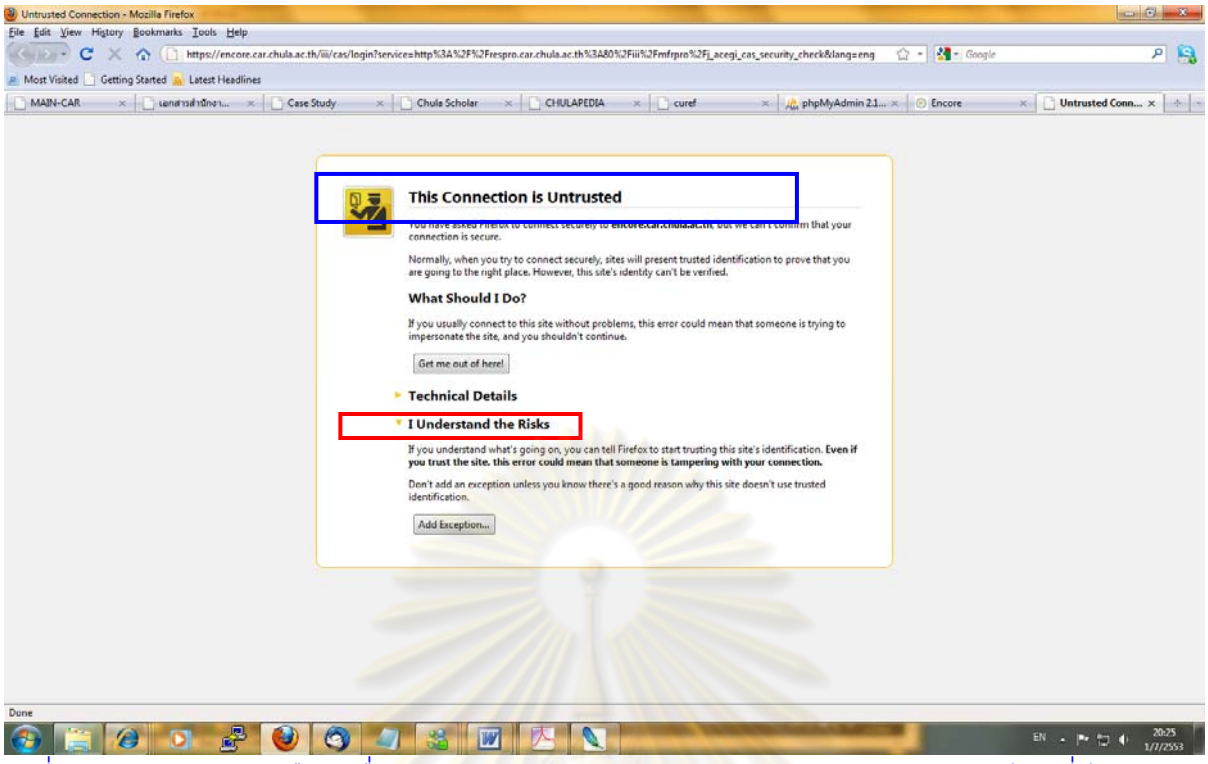
* บรรณารักษ์ฝ่ายระบบสารสนเทศ ศูนย์วิทยทรัพยากร จุฬาลงกรณ์มหาวิทยาลัย

ก็จะสามารถเห็นเป็นตัว A ได้โดยง่าย ทำให้เกิดความไม่ปลอดภัยในการใช้งานในครั้งต่อ ๆไปได้ เป็นต้น และหากยังคงมีการใช้ http:// เพื่อการแสดงตนนี้ก็อาจจะเกิดการลักลอบเข้าใช้ระบบได้โดยง่าย ผู้ให้บริการจึงปรับปรุงการติดต่อกับสมาชิกผู้เข้าใช้ระบบอินเตอร์เน็ตเป็นโพรโทคอลมาตรฐานอีกแบบหนึ่งที่ เรียกว่า HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) หรือที่เรียกย่อ ๆ ว่า HTTP over SSL ซึ่งเป็นเทคนิคการเข้ารหัสข้อมูลก่อนที่จะส่งจากเครื่องคอมพิวเตอร์ของผู้ใช้ไปยังเครื่องแม่ข่ายของผู้ให้บริการ การเข้ารหัสข้อมูลนี้ทำให้ข้อมูลที่จะส่งผ่านอยู่ในรูปที่ไม่สามารถอ่านออกได้ในทันที ผู้มีสิทธิ์ที่แท้จริงเท่านั้นจึงจะมีกุญแจสามารถถอดรหัสเพื่ออ่านข้อมูลนั้นได้ ถึงแม้จะมีการลักลอบขโมยไปได้ ผู้อื่นก็ไม่สามารถนำมาใช้ประโยชน์ได้ ระบบมาตรฐานนี้จึงเป็นการเพิ่มความปลอดภัยทางอินเทอร์เน็ตได้ทางหนึ่ง เทคนิคการเข้ารหัสดังกล่าวได้มีการนำมาใช้อย่างแพร่หลายในการแสดงตนของสมาชิกเพื่อเข้าใช้บริการของแต่ละหน่วยงานทั้งที่เป็นภาครัฐและเอกชน เช่น ธุรกรรมทางการเงินผ่านออนไลน์ ของธนาคารต่าง ๆ ที่ผู้ใช้บริการต้องแสดงตนก่อนการเข้าไปทำธุรกรรมทางการเงิน เป็นต้น

ด้วยเทคนิคการเข้ารหัสแบบนี้ อาจก่อให้เกิดปัญหาที่พบหน้าจอแสดงการเตือนให้ผู้ใช้ระวังเรื่องความปลอดภัย เนื่องจากเว็บเบราว์เซอร์ที่ผู้ใช้ใช้งานอยู่ในขณะนั้นไม่สามารถตรวจสอบหาชื่อหน่วยงานที่รับรองการเข้ารหัสนี้จากรายชื่อในTrusted Root Certification Authorities ที่แนบมากับเว็บเบราว์เซอร์ได้ เช่น เว็บเบราว์เซอร์ Internet Explorer (IE) จะแสดงหน้าต่างเตือนให้ผู้ใช้ ด้วยข้อความ “There is a problem with this website’s security certificate” ส่วนเว็บเบราว์เซอร์ Mozilla Firefox จะแสดงหน้าต่างเตือนให้ผู้ใช้ ด้วยข้อความ “This Connection is Untrusted” เพื่อให้ผู้ใช้ยืนยันจะเปิดหน้าเว็บดังกล่าวก่อน แทนการเปิดหน้าเว็บไซต์ที่ผู้ใช้ต้องการให้ในทันที ดังภาพที่ 1 และภาพที่ 2 ตามลำดับ

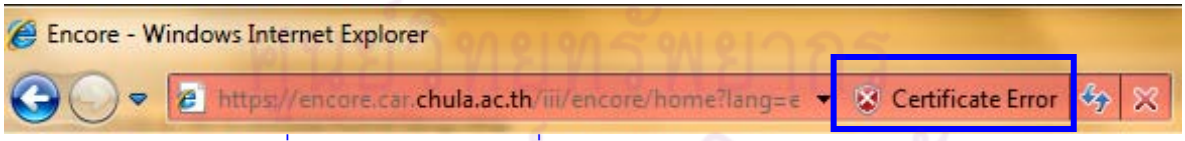


ภาพที่ 1 ตัวอย่างหน้าต่างเตือน เมื่อใช้ผ่านเว็บเบราว์เซอร์ IE และพบหน้าเว็บไซต์ที่มีการเข้ารหัส SSL โดยเว็บบราว์เซอร์ไม่สามารถตรวจสอบหน่วยงานที่รับรองการเข้ารหัสได้

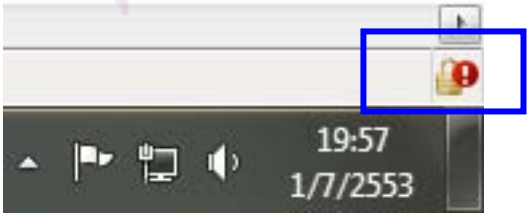


ภาพที่ 2 ตัวอย่างหน้าต่างเตือน เมื่อใช้ผ่านเว็บเบราว์เซอร์ Mozilla Firefox และพบหน้าเว็บไซต์ที่มีการเข้ารหัส SSL ซึ่งเว็บบราว์เซอร์ไม่สามารถตรวจสอบหน่วยงานที่รับรองการเข้ารหัสได้

จากหน้าต่างเตือน ผู้ใช้สามารถเข้าไปในหน้า เว็บไซต์ ที่ต้องการจะเปิดได้ โดยคลิกที่ “Continue to this website (Not recommended)” ในเว็บเบราว์เซอร์ IE หน้าต่างในภาพที่ 1 หรือคลิกที่ “I understand the risk” ใน เว็บเบราว์เซอร์ Mozilla Firefox หน้าต่างในภาพที่ 2 เพื่อยืนยันจะเปิดหน้าเว็บไซต์ดังกล่าว และเมื่อเข้าไปเว็บไซต์นั้น ๆได้ โดยเมื่อเข้าไปแล้วจะมีข้อความ Certificate Error ที่ Address Bar มุมบนด้านขวาของเว็บเบราว์เซอร์ IE ดังภาพที่ 3 หรือพบเครื่องหมายตกใจสีแดงบนรูปกุญแจซึ่งหมายถึง Certificate Error ที่มุมล่างด้านขวาของเว็บเบราว์เซอร์ Mozilla Firefox ดังภาพที่ 4



ภาพที่ 3 Certificate error ที่ Address bar ของ เว็บเบราว์เซอร์ IE



ภาพที่ 4 ภาพเครื่องหมายตกใจสีแดงบนรูปกุญแจ มุมล่างขวาของเบราว์เซอร์ Mozilla Firefox

ทำอย่างไรไม่ให้มี Certificate Error

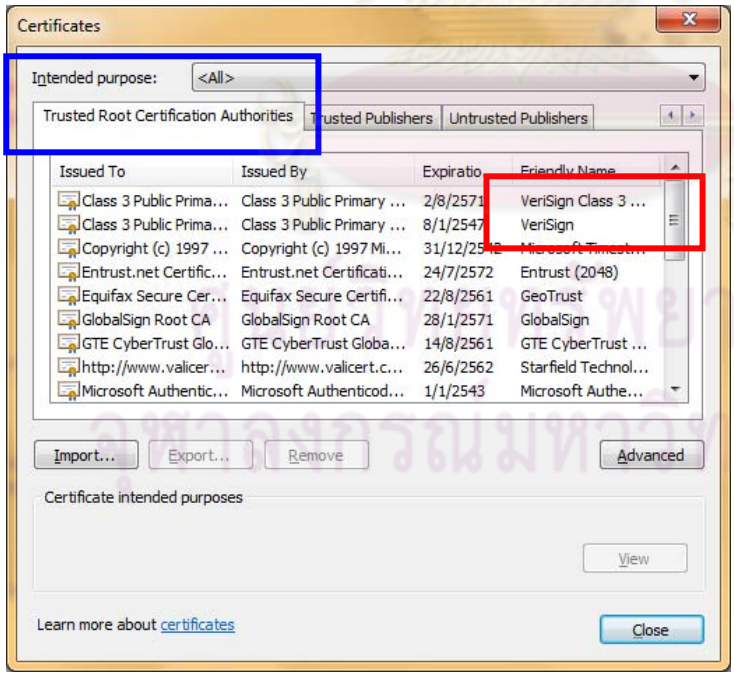
Certificate Error เกิดจากการที่เว็บเบราว์เซอร์ไม่สามารถตรวจสอบหาใบรับรองหน่วยงานผู้เป็นเจ้าของเว็บไซต์นี้จากรายชื่อในTrusted Root Certification Authorities ที่แนบมากับเว็บเบราว์เซอร์ได้ ดังนั้นหน่วยงานเจ้าของเว็บไซต์จะต้องมีใบรับรองอิเล็กทรอนิกส์เพื่อการแก้ไขปัญหานี้

ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) หมายถึง ข้อมูลอิเล็กทรอนิกส์ที่ออกโดยผู้ให้บริการออกใบรับรอง (Certification Authority) เพื่อใช้บ่งบอกถึงความมีตัวตนที่แท้จริง และรับรองข้อมูลต่าง ๆ ซึ่งรวมถึงกุญแจสาธารณะที่ปรากฏในใบรับรองอิเล็กทรอนิกส์ว่าเป็นของบุคคลนั้นจริง โดยอาศัยเทคโนโลยีที่เรียกว่าเทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure) (ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ 2550 :14) การมีใบรับรองอิเล็กทรอนิกส์ที่อยู่ในรายการของ Trusted Root Certification Authorities ของ เว็บเบราว์เซอร์นั้นจะช่วยให้ไม่มี Certificate Error บนหน้าจอเว็บไซต์ ทั้งนี้เจ้าของผู้ให้บริการเว็บไซต์ สามารถดำเนินการเพื่อการมีใบรับรองนี้ได้ใน 2 ลักษณะ คือ

1. ผู้ให้บริการเว็บไซต์ใช้บริการจากบริษัทผู้ให้บริการทำใบรับรองอิเล็กทรอนิกส์
2. ผู้ให้บริการเว็บไซต์ทำใบรับรองอิเล็กทรอนิกส์ขึ้นมาใช้เอง

รายละเอียดมีดังนี้

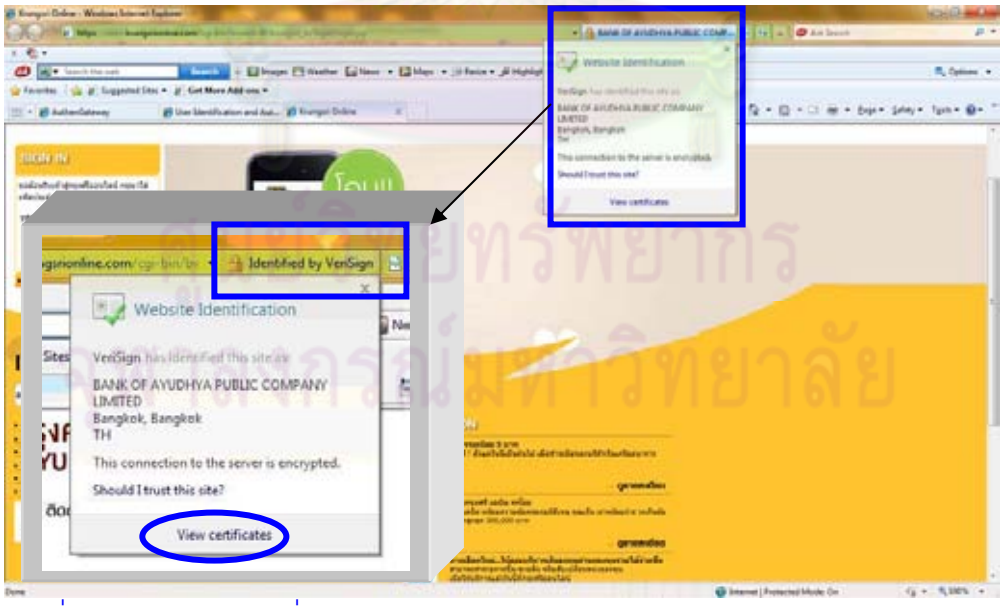
1.ผู้ให้บริการเว็บไซต์ใช้บริการจากบริษัทผู้ให้บริการทำใบรับรองอิเล็กทรอนิกส์ เช่น จากบริษัท VeriSign ซึ่งมีรายชื่ออยู่ใน Trusted Root Certification Authorities ของเว็บเบราว์เซอร์ IE ดังปรากฏในภาพที่ 5



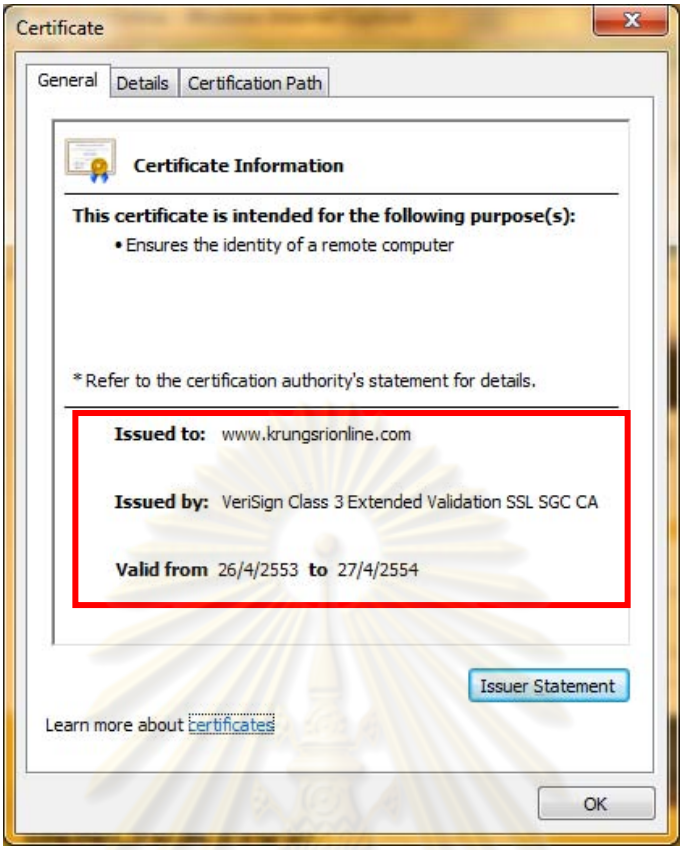
ภาพที่ 5 ชื่อบริษัท VeriSign ผู้ให้บริการออกใบรับรอง ปรากฏในรายชื่อ Trusted Root Certification Authorities ของเบราว์เซอร์ IE

โดยบริษัทผู้ให้บริการทำใบรับรองอิเล็กทรอนิกส์นี้ จะทำหน้าที่เป็นตัวกลางในการตรวจสอบความมีตัวตนและความน่าเชื่อถือของเว็บไซต์ของผู้ขอมีใบรับรอง โดยบริษัทจะรับคำร้องขอจากผู้ขอ และส่งมอบใบรับรองให้กับเจ้าของ เว็บไซต์ เพื่อนำใบรับรองนั้นไปติดตั้งในเครื่องแม่ข่ายที่ให้บริการเว็บไซต์ หลังจากมีการติดตั้งใบรับรองเรียบร้อยแล้ว จะเป็นผลให้เว็บเบราว์เซอร์สามารถแสดงหน้าจอเว็บไซต์ที่ต้องการได้โดยทันที เมื่อผู้ใช้บริการคลิกเพื่อเข้าใช้บริการผ่าน HTTPS ของ เว็บไซต์นั้น ๆ

ในปัจจุบันเราจะพบว่า หน่วยงานต่าง ๆ ที่มีกิจกรรมเกี่ยวข้องกับการทำธุรกรรมทางการเงินนิยมขอใบรับรองอิเล็กทรอนิกส์จากบริษัทผู้ให้บริการออกใบรับรองนี้ เพื่อให้ผู้ใช้มั่นใจในการเข้าใช้บริการผ่านหน้าเว็บไซต์ที่มีการเข้ารหัส อาทิ ธนาคารกรุงศรีอยุธยา จำกัด ธนาคารกรุงเทพ จำกัด ใช้บริการขอใบรับรองจากบริษัท VeriSign เมื่อผู้ใช้บริการคลิกเรียกใช้บริการหน้าเว็บไซต์ของธนาคารเหล่านี้ในส่วนของการทำธุรกรรมทางการเงิน จะพบหน้าจอ https:// เพื่อให้ผู้ใช้พิมพ์ User ID และ Password โดยทันที ตัวอย่างหน้าเว็บไซต์ของธนาคารกรุงศรีอยุธยา จำกัด เมื่อคลิกเลือกที่**กรุงศรีออนไลน์** บนหน้าเว็บไซต์จะเชื่อมโยงไปที่ https://www.krungsrionline.com/cgi-bin/bvisapi.dll/krungsri_ib/login/login.jsp โดยผู้ใช้จะพบเพิ่มเติมว่าที่หน้าเว็บไซต์นี้มีสัญลักษณ์รูปกุญแจสีเหลืองพร้อมชื่อบริษัทผู้ออกใบรับรองอิเล็กทรอนิกส์แทนข้อความ Certificate Error ในบริเวณ Address Bar ของเว็บเบราว์เซอร์ตลอดเวลาที่เราเข้าใช้เว็บไซต์นี้ เมื่อนำเมาส์คลิกที่รูปกุญแจสีเหลือง จะมีข้อความแสดงว่า URL นี้ใช้บริการขอการรับรองจากบริษัท VeriSign ดังภาพที่ 6 และเมื่อคลิกที่ View Certificates จะพบหน้าจอแสดงการรับรองจากบริษัท VeriSign ดังปรากฏในภาพที่ 7 ตามลำดับ



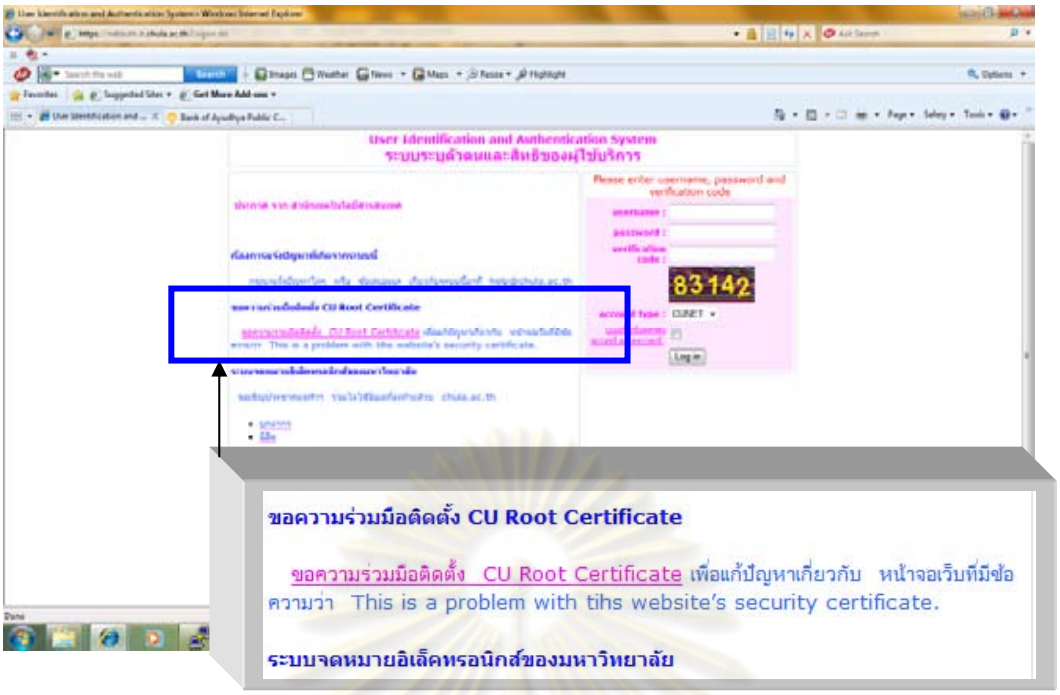
ภาพที่ 6 หน้าต่างเว็บไซต์ที่มีรูปกุญแจสีเหลืองแสดงการเข้ารหัส SSL และได้รับการรับรอง



ภาพที่ 7 หน้าจอแสดงการรับรองจากบริษัท VeriSign ที่ให้กับเว็บไซต์

2. ผู้ให้บริการเว็บไซต์ทำใบรับรองอิเล็กทรอนิกส์ขึ้นมาใช้บนเครื่องแม่ข่ายของตนเอง และให้สมาชิกของตนนำโปรแกรม CA Rootไปติดตั้งในเว็บเบราว์เซอร์ของเครื่องคอมพิวเตอร์ลูกข่ายที่ต้องการใช้บริการ เพื่อทำให้เว็บเบราว์เซอร์นั้น ๆ รู้จักผู้ให้บริการใบรับรองเพิ่มเติม วิธีนี้เป็นที่นิยมนำมาใช้ในหน่วยงานที่ไม่เกี่ยวข้องกับธุรกรรมทางการเงิน ทั้งนี้การเข้ารหัสหน้าเว็บไซต์ให้บริการเครือข่ายอินเทอร์เน็ตที่มีเพื่อให้ผู้ใช้บริการแสดงตนด้วยการพิมพ์ Username และ Password ก่อนการเข้าใช้ระบบเครือข่ายขององค์กร เพื่อการเก็บข้อมูลการเข้าใช้งานเท่านั้น

ตัวอย่างหน่วยงานที่ทำใบรับรองขึ้นมาใช้เพื่อรับรองตนเอง อาทิ สำนักเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย ได้นำวิธีการนี้มาใช้เพื่อการให้แก่ผู้ที่ต้องการใช้บริการเครือข่ายคอมพิวเตอร์จากสำนักฯ เพื่อใช้ระบบเครือข่ายของมหาวิทยาลัยเพื่อเชื่อมโยงออกไปยังที่ต่าง ๆ ผ่านอินเทอร์เน็ต โดยผู้เข้าใช้บริการจะพบหน้าจอ https://netauth.it.chula.ac.th/ ซึ่งมีคำแนะนำในการติดตั้ง CU Root Certificate ดังภาพที่ 8

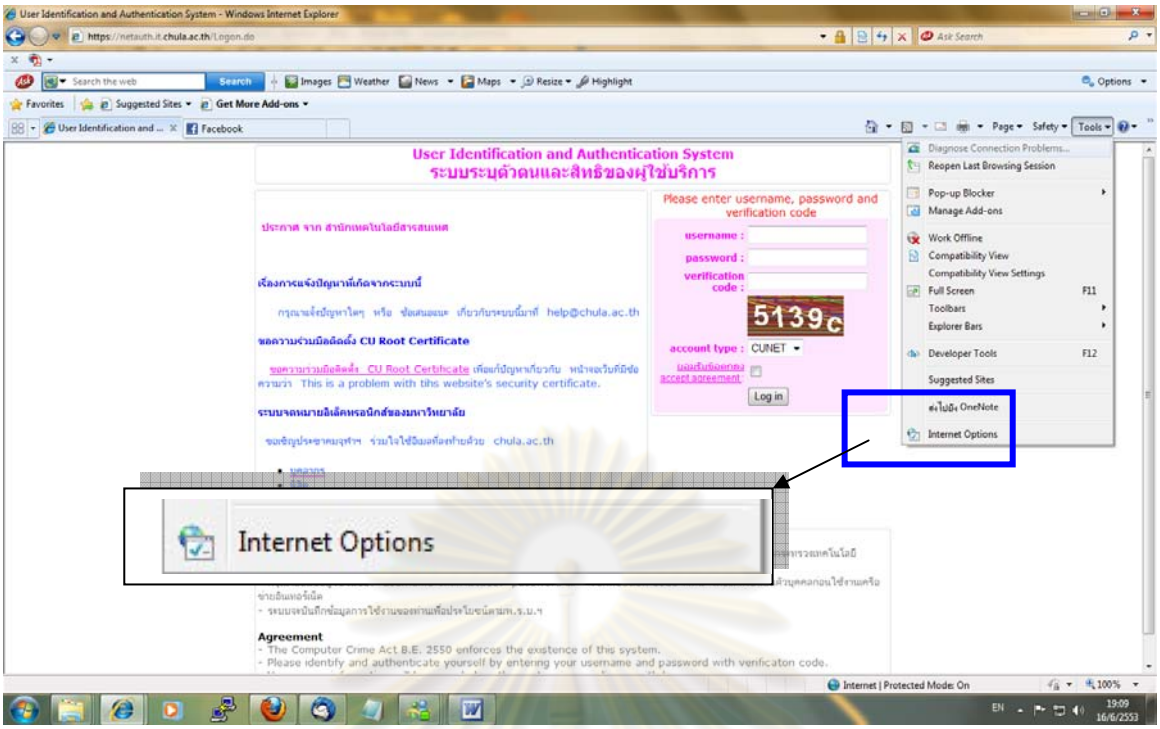


ภาพที่ 8 หน้าเว็บไซต์ของจุฬาฯ เพื่อการแสดงตนก่อนการเข้าใช้ระบบอินเทอร์เน็ต พร้อมคำแนะนำให้ใช้บริการติดตั้ง CU Root Certificate

สำหรับผู้เข้าใช้บริการเครือข่ายจุฬาลงกรณ์มหาวิทยาลัย ควรติดตั้ง CU Root Certificate ลงบนคอมพิวเตอร์ที่ต้องการใช้งาน เพื่อจะไม่ต้องพบหน้าต่างเตือนดังที่ปรากฏในภาพที่ 1 ให้เกิดความรำคาญอีกต่อไป ประโยชน์สืบเนื่องจากการติดตั้ง CU CA Root นี้ นอกจากจะใช้สำหรับการเข้ารหัสหน้าเว็บไซต์เพื่อการแสดงตัวตนก่อนการเข้าใช้อินเทอร์เน็ตของมหาวิทยาลัยแล้ว ยังครอบคลุมทุกหน้าเว็บไซต์ที่มีการเข้ารหัสภายใต้โดเมน chula.ac.th อีกด้วย กล่าวคือ เมื่อติดตั้งเรียบร้อยแล้วผู้ใช้สามารถเข้าใช้ทุกหน้าเว็บไซต์ที่มีการเข้ารหัสของทุกหน่วยงานของจุฬาฯ อาทิ หน้าเว็บไซต์ที่ต้อง Login เพื่อเข้าใช้ระบบอิเล็กทรอนิกส์เมลของมหาวิทยาลัย (https://webmail.it.chula.ac.th/) หน้าเว็บเพื่อการลงทะเบียนการเข้าใช้เครือข่ายไร้สาย Nirasnet (https://radius2.it.chula.ac.th/wlan/) เป็นต้น

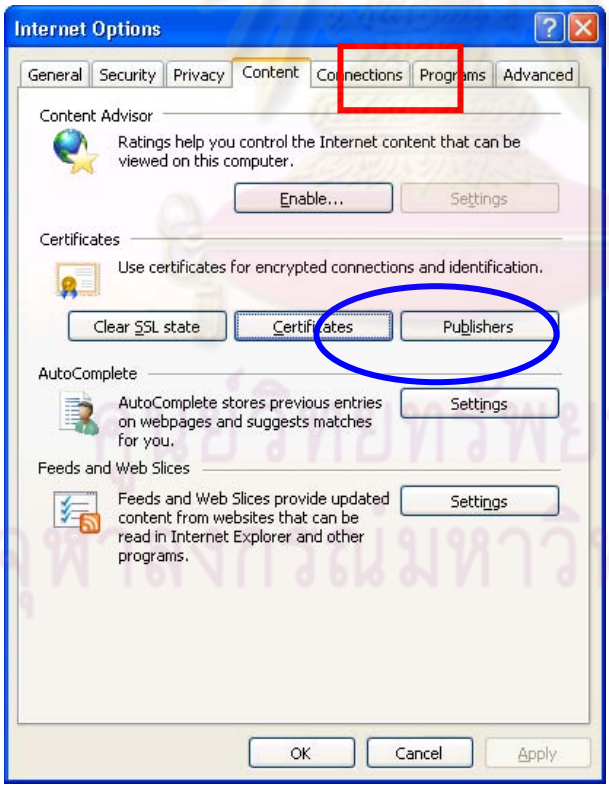
การตรวจสอบรายชื่อผู้ให้บริการ Certification Authority ในเว็บเบราว์เซอร์

ผู้ใช้สามารถตรวจดูรายชื่อผู้ให้บริการ Certification Authority ได้จากเว็บเบราเซอร์ที่ใช้งาน เช่น ในเว็บเบราว์เซอร์ IE ทำได้โดยคลิกที่ Tools -> Internet Options แล้วเลือกคลิกที่ ดังภาพที่ 9



ภาพที่ 9 ภาพหน้าจอเว็บเบราว์เซอร์ IE เพื่อการตรวจดูรายชื่อผู้ให้บริการ Certification Authority

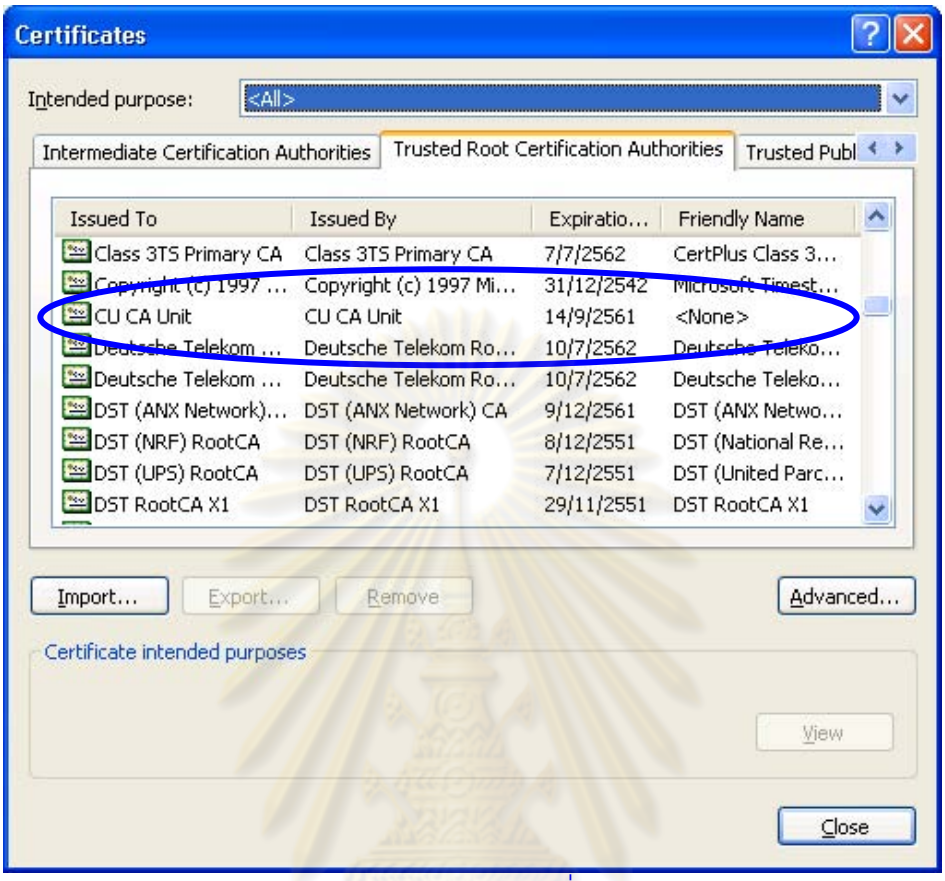
จากนั้นเลือกที่แถบ Content ลำดับถัดมา และคลิกเลือกที่ปุ่ม Certificates ดังภาพที่ 10



ภาพที่ 10 หน้าจอ Content
คลิกเลือกปุ่ม Certificates

เมื่อคลิก Certificates จะพบรายละเอียดของผู้ให้บริการ (Certification Authority) ที่มีการติดตั้งในเว็บเบราว์เซอร์นี้เรียบร้อยแล้ว โดยอาจจะมาพร้อมเว็บเบราว์เซอร์ หรือเกิดจากการที่ผู้ใช้เว็บเบราว์เซอร์นี้ได้ติดตั้งโปรแกรม CA Root บนคอมพิวเตอร์เครื่องนี้ดังที่กล่าวในข้อ 2 ข้างต้น เช่นเมื่อผู้ใช้บริการติดตั้ง CU Root

Certificate ลงบนคอมพิวเตอร์ที่ต้องการใช้งาน จะพบ CU CA Unit ปรากฏในรายชื่ออยู่ใน Trusted Root Certification Authorities ของเว็บเบราว์เซอร์ IE ด้วย ดังตัวอย่างหน้าจอในภาพที่ 11



ภาพที่ 11 หน้าจอภาพ CU CA Unit ในรายการ Certificates ที่มีใน Trusted Root Certification Authorities ของ เว็บเบราว์เซอร์ IE

ข้อสรุปและเสนอแนะ

ใบรับรองอิเล็กทรอนิกส์สำหรับการให้บริการเครื่องแม่ข่ายที่มีการเข้ารหัสนี้ เป็นการยืนยันว่า เว็บไซต์นี้เปิดให้บริการโดยหน่วยงานหรือองค์กรที่จดทะเบียนถูกต้องและมีตัวตนอยู่จริง เป็นการให้ความมั่นใจแก่ผู้เข้ารับบริการผ่านหน้าเว็บไซต์ที่มีการเข้ารหัส (HTTPS) รู้สึกปลอดภัยในการเข้าทำกิจกรรมในหน้าเว็บไซต์เหล่านี้ เช่น การรับส่งอีเมล การเข้าไปลงทะเบียนเรียน การเข้าไปทำธุรกรรมทางการเงินผ่านระบบออนไลน์ ฯลฯ

หน่วยงานที่มีการทำใบรับรองอิเล็กทรอนิกส์ขึ้นมาใช้ด้วยตัวเองนั้น ควรให้ความสำคัญกับการประชาสัมพันธ์เพื่อทำความเข้าใจเรื่องระบบการเข้าใช้งานหน้าเว็บไซต์ที่มีการเข้ารหัสของหน่วยงาน ตลอดจนประโยชน์ของการติดตั้ง CA Root ของหน่วยงานลงในเว็บเบราว์เซอร์ที่ใช้ประจำให้กับผู้รับบริการของตนทราบด้วย เพราะหากผู้รับบริการไม่ปฏิบัติตาม จะส่งผลให้เว็บเบราว์เซอร์แสดงหน้าจอเตือนผู้ใช้ทุกครั้งที่มีการเรียกใช้หน้าเว็บไซต์ที่มีการเข้ารหัสของหน่วยงาน

จากประสบการณ์ผู้เขียนพบว่า ห้องสมุดมหาวิทยาลัยหลายแห่งให้บริการสืบค้นผ่านหน้าเว็บไซต์ เพื่อการสืบค้นแบบครั้งเดียวในเวลาเดียวกัน(Single Search / Federated Search) ไปยังทุก ๆ ฐานข้อมูลของ

ห้องสมุดและฐานข้อมูลออนไลน์ต่าง ๆที่ห้องสมุดบอกรับไว้ ห้องสมุดจำเป็นต้องมีหน้าเว็บไซต์ที่มีการเข้ารหัสเพื่อให้ผู้ใช้บริการแสดงตัวตนและพิสูจน์สิทธิ์ก่อนการเข้าใช้บริการ บางครั้งใบรับรองอิเล็กทรอนิกส์ที่หน่วยงานทำขึ้นเพื่อใช้บนเครื่องแม่ข่ายด้วยตนเองอาจไม่รองรับกับโปรแกรมการสืบค้นสำเร็จรูปเช่นนี้ เพื่ออำนวยความสะดวกแก่ผู้ใช้บริการในการเข้าใช้บริการสืบค้นข้อมูลได้อย่างสมบูรณ์ห้องสมุดควรเตรียมงบประมาณเพื่อการมีใบรับรองอิเล็กทรอนิกส์โดยใช้บริการจากบริษัทผู้ให้บริการทำใบรับรองอิเล็กทรอนิกส์ มิฉะนั้นผู้ใช้บริการหน้าเว็บไซต์ของห้องสมุดพบการแจ้งเตือนทุกครั้งที่มีการเรียกใช้หน้าเว็บไซต์นี้ การที่พบหน้าจอเตือนบ่อยครั้งอาจจะส่งผลให้ผู้รับบริการของหน่วยงานขาดความเชื่อมั่นในหน่วยงานนั้น ๆและไม่สนใจจะเข้าใช้บริการต่อไป

หมายเหตุ

ขอขอบพระคุณ คุณชยา ลิมจิตติ รักษาการผู้อำนวยการ สำนักเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย. และ คุณเรืองศรี จุลละจินดา หัวหน้าฝ่ายบริการช่วยค้นคว้าวิจัย ศูนย์วิทยทรัพยากร จุฬาลงกรณ์มหาวิทยาลัย ในการอ่านบทความและให้คำแนะนำต่าง ๆ เป็นอย่างดี

บรรณานุกรม

ธนาคารกรุงศรีอยุธยา จำกัด. [ออนไลน์]. เข้าถึงได้จาก https://www.krungsrionline.com/cgi-bin/bvisapi.dll/krungsri_ib/login/login.jsp สืบค้นวันที่ 1 มิถุนายน 2553.

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. 2550. “สรุปการเสวนารับฟังความคิดเห็นร่างพ.ร.ฎ.กำกับดูแลผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (CA) และนโยบายการออกใบรับรอง (CP) และแนวทางปฏิบัติ (CPS) ของผู้ประกอบการ "ความน่าเชื่อถือของ CA ไย กับความมั่นใจของธุรกรรมออนไลน์" ” [ออนไลน์]. เข้าถึงได้จาก http://www.etcommission.go.th/documents/ca/2007_03_09/20070309_ca_result_note.pdf สืบค้นวันที่ 19 มิถุนายน 2553.

สมใจ บุญศิริ. บรรณาธิการ. อินเตอร์เน็ต : นานาสาระแห่งการบริการ = Internet : variety services. กรุงเทพฯ : สถาบันวิทยบริการ จุฬาลงกรณ์มหาวิทยาลัย, 2538.

สำนักเทคโนโลยีสารสนเทศ. จุฬาลงกรณ์มหาวิทยาลัย. [ออนไลน์] เข้าถึงได้จาก https://netauth.it.chula.ac.th/ สืบค้นวันที่ 15 มิถุนายน 2553.