การลดค่าใช้จ่ายในการรักษาความปลอดภัยของเว็บไซต์ด้วย Let's Encrypt: กรณีศึกษามหาวิทยาลัยราชภัฏอุดรธานี

REDUCING WEBSITE SECURITY COSTS WITH LET'S ENCRYPT: A CASE STUDY OF UDON THANI RAJABHAT UNIVERSITY

นิธิเวทย์ เจียมวิจิตร
ศูนย์คอมพิวเตอร์ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏอุดรธานี
Nithiwet Jiamwijit
Computer Center, Office of Academic Resource and Information Technology,
Udon Thani Rajabhat University

(Received: May 22, 2024; Revised: July 4, 2024; Accepted: September 18, 2024)

*ผู้ประสานงาน : นายนิธิเวทย์ เจียมวิจิตร อีเมล : nitiwate@udru.ac.th

บทคัดย่อ

การรักษาความปลอดภัยของเว็บไซต์เป็นเรื่องสำคัญอย่างมากในยุคที่เทคโนโลยีอินเทอร์เน็ตและการสื่อสารมีบทบาทสำคัญในชีวิตประจำวันของเรา การใช้งานเว็บไซต์ที่มีการสื่อสารผ่านทางอินเทอร์เน็ตมีแนวโน้มที่จะเพิ่มขึ้นอย่างต่อเนื่อง แต่ช่องทางการสื่อสารผ่านทางอินเทอร์เน็ตก็มีความเสี่ยงสูงเช่นกัน เนื่องจากผู้ไม่ประสงค์ดีพยายามค้นหาช่องโหว่ต่างๆ เพื่อดักจับข้อมูลซึ่งอาจจะทำให้เกิดความสูญเสียตามมาได้ ดังนั้นการรักษาความปลอดภัยของเว็บไซต์ จึงมีความสำคัญในการป้องกันการเข้าถึงข้อมูล มหาวิทยาลัยราชภัฏอุดรธานี ได้มีการใช้ SSL/TLS certificates ในการรักษาความปลอดภัยเว็บไซต์ของมหาวิทยาลัยที่บริการแก่บุคลากร นักศึกษา และบุคคลทั่วไป ซึ่งจำเป็นอย่างยิ่งต่อมหาวิทยาลัยในการสื่อสารข้อมูลกับภายนอก จึงได้ใช้บริการและเสียค่าใช้บริการดังกล่าว จากผู้ให้บริการมาแล้วหลายปี จากเหตุดังกล่าว มหาวิทยาลัยจึงได้หาทางลดค่าใช้จ่ายโดยการใช้ SSL/TLS certificates ของ Let's Encrypt เนื่องจาก Let's Encrypt เป็นบริการที่ให้ใบรับรอง SSL/TLS โดยไม่เสียค่าใช้จ่าย พร้อมทั้งประสิทธิภาพของ certificate ของ Let's Encrypt ที่เทียบเท่ากับแบบซื้อจากผู้ให้บริการ จึงเป็นทางเลือกที่เหมาะสมสำหรับใช้ในมหาวิทยาลัย

คำสำคัญ: เฮชทีทีพีเอส, เลเยอร์ซ็อกเก็ตที่ปลอดภัย, เอสเอสแอล/ทีแอลเอส, เล็ทสเอ็นคริปต์, ลดค่าใช้จ่าย

ABSTRACT

Website security is of paramount importance in the age of the internet and communication technology playing a significant role in our daily lives. The use of websites with internet communication is likely to increase continuously, but internet communication channels also have high risks. This is because ill-intentioned individuals try to find loopholes to intercept data, which may lead to losses. Therefore, website security is crucial in preventing unauthorized access to data. Udon Thani Rajabhat University has been using SSL/TLS certificates to secure its website, which provides services to its staff, students, and the public. As communication with external parties is essential for the university, it has been using and paying for such services from private companies for many years. To reduce costs, the university has decided to explore using Let's Encrypt's SSL/TLS certificates. Let's Encrypt is a service that provides SSL/TLS certificates free of charge. The performance of Let's Encrypt's certificates is comparable to that of private companies, making it a suitable option for the university.

Keywords: HTTPS, Secure Socket Layer, SSL/TLS, Let's Encrypt, Reduce cost.

1. บทนำ

ในปัจจุบัน เว็บไซต์มีความสำคัญอย่างยิ่งต่อการดำเนินงานของมหาวิทยาลัยราชภัฏอุดรธานี เว็บไซต์ของมหาวิทยาลัยเป็นช่องทางหลักในการสื่อสารข้อมูล ข่าวสาร กิจกรรม บริการต่างๆ ไปยังนักศึกษา บุคลากร และประชาชนทั่วไป ในปัจจุบันช่องทางการใช้เว็บไซต์มีความเสี่ยงสูง เนื่องจากมีผู้ไม่ประสงค์ดี พยายามค้นหาช่องโหว่ต่างๆ เพื่อดักจับข้อมูลต่างๆ ซึ่งอาจจะทำให้เกิดความสูญเสียตามมาได้ ดังนั้น เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นผ่านการใช้เว็บไซต์ การใช้ ใบรับรองอิเล็กทรอนิกส์ (SSL/TLS certificates) จึงเป็นทางเลือกหนึ่งในการปกป้องข้อมูลระบบรักษาความปลอดภัยของเว็บไซต์

SSL ย่อมาจาก Secure Socket Layer [1] ซึ่งปัจจุบันได้พัฒนาขึ้นมาเป็น TLS (Transport Layer Security) [2] คือ เทคโนโลยีการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ตระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์ เพื่อให้ข้อมูลปลอดภัยจากการเข้าถึงข้อมูลจากผู้ไม่ประสงค์ดี TLS จะทำงานผ่านโปรโตคอลที่เป็นที่นิยมใช้อย่าง HTTPS เพื่อทำงานร่วมกับ SSL/TLS certificates ที่เป็นไฟล์ข้อมูลขนาดเล็กที่เครื่องเซิร์ฟเวอร์ เพื่อยืนยันตัวตนและความถูกต้องในการส่งข้อมูลระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์ ซึ่งมีการเข้ารหัสและ

ถอดรหัสผ่านเทคโนโลยี SSL/TLS หากข้อมูลถูกดักจับไปได้ ข้อมูลก็ยังมีความปลอดภัย เพราะจะไม่สามารถถอดรหัสข้อมูลได้ ซึ่ง SSL/TLS certificates จะมีทั้งแบบที่ต้องซื้อผ่านผู้ให้บริการและแบบที่ไม่มีค่าใช้จ่ายจากองค์กรไม่แสวงหาผลกำไร

มหาวิทยาลัยราชภัฏอุดรธานี ได้มีการใช้ SSL/TLS certificates ในการรักษาความปลอดภัยของเว็บไซต์ของมหาวิทยาลัยที่บริการแก่บุคลากร นักศึกษา และบุคคลทั่วไป ซึ่งจำเป็นอย่างยิ่งต่อมหาวิทยาลัยในการสื่อสารข้อมูลกับภายนอก จึงได้ใช้บริการและเสียค่าใช้บริการดังกล่าว จากผู้ให้บริการมาแล้วหลายปี เนื่องจากมีการสนับสนุนทางเทคนิคจากทางผู้ให้บริการ ผู้วิจัยจึงได้ทดลองใช้ SSL/TLS certificates ของ Let’s Encrypt จากองค์กรไม่แสวงหาผลกำไร เพื่อลดค่าใช้จ่ายดังกล่าว

ดังนั้นในงานวิจัยนี้จึงเสนอแนวทางในการลดค่าใช้จ่ายในการซื้อ SSL/TLS certificates โดยมีการศึกษาและวิเคราะห์ประสิทธิภาพ SSL/TLS certificates ของ Let's Encrypt เปรียบเทียบกับการใช้ SSL/TLS certificates จากผู้ให้บริการแบบเดิมที่ต้องมีค่าใช้จ่ายในการต่ออายุทุกปี เพื่อนำมาช่วยในการลดค่าใช้จ่ายในการรักษาความปลอดภัยของเว็บไซต์ของมหาวิทยาลัย

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1. Secure Socket Layer (SSL)

ถูกพัฒนาขึ้นโดยบริษัทเน็ตสเคป (Netscape Communications) ในปี ค.ศ.1994 เพื่อเป็นโพรโทคอลที่ให้บริการสำหรับการเข้ารหัสข้อมูลและการพิสูจน์ตัวตนในการสื่อสารระหว่างเซิร์ฟเวอร์ (Server) และไคลเอนท์ (Client) ทำให้การสื่อสารมีความปลอดภัยมากยิ่งขึ้น ซึ่งปกติแล้วข้อมูลที่ส่งไปมาระหว่างกันจะไม่มีการเข้ารหัสข้อมูลทำให้การดักจับข้อมูลเป็นไปได้โดยง่ายต่อมา SSL [1] เวอร์ชั่น 3.0 ในปี ค.ศ. 1997 ได้ถูกทำการทดสอบแล้วพบว่าไม่มีความปลอดภัยในการใช้งาน จึงมีการพัฒนา SSL ให้เกิดเป็นมาตรฐานกลางของโพรโทคอลบนอินเทอร์เน็ตที่นำไปสู่การออกแบบ Transport Layer Security (TLS) [2] ที่ถูกกำหนดให้เป็นมาตรฐานอย่างเป็นทางการ ในปี ค.ศ. 1999 โดยเป็นมาตรฐานการสื่อสารของ Internet Engineering Task Force (IETF) แต่โพรโทคอล TLS นั้นจะมีความแตกต่างจาก SSL เพียงเล็กน้อย โดยส่วนที่แตกต่างกันก็คือ Version, Cipher Suite, Alert Protocol, Handshake Protocol และ Record Protocol เป็นต้น ปัจจุบัน TLS ถูกพัฒนามาถึงเวอร์ชัน 1.3 ซึ่งเริ่มมีการใช้งานมาตั้งแต่ปี ค.ศ.2018

2.2 HTTP Over TLS (HTTPS) [3]

Transport Layer Security (TLS) ที่เป็นโพรโทคอลที่ทำงานในระดับของ Transport Layer ในการนำใช้งานจึงนำมาประยุกต์ใช้กับโพรโทคอลระดับแอปพลิเคชัน เช่น IMAP, POP3, LDAP, SSH และ FTP เป็นต้น รวมถึงการนำ TLS มาประยุกต์ใช้กับโปรแกรมประยุกต์เว็บ โดยปกติ เว็บไซต์ทั่วไปจะใช้โพรโทคอล HTTP [4] ในการสื่อสารข้อมูลระหว่างกัน ข้อมูลที่รับส่งจะอยู่ในรูปแบบของ

ข้อความปกติ (Clear Text) ที่มีความเสี่ยงต่อการถูกโจมตีด้วยการดักจับข้อมูล (Sniffing) จึงมีการเสนอให้นำ TLS มาประยุกต์ใช้ร่วมกับ HTTP เพื่อสร้างเป็นการสื่อสารรูปแบบใหม่ขึ้นเรียกว่า HTTP Over TLS (HTTPS) เกิดจากแนวความคิดในการสร้างช่องทางการสื่อสารข้อมูลบนเว็บไซต์ที่มีการเข้ารหัสเพื่อความปลอดภัยในระหว่างการใช้งานเว็บไซต์ ซึ่งบนโพรโทคอล HTTPS นี้ เว็บเบราว์เซอร์จะแสดง URL ของเว็บไซต์ ตัวอย่างเช่น https://www.udru.ac.th แทนซึ่งเดิม ในโพรโทคอล HTTP ที่เคยใช้งานนั้น URL คือ http://www.udru.ac.th

2.3 Let's Encrypt

Let's Encrypt เป็นระบบหน่วยงานออกใบรับรอง (Certification Authority หรือ CA) ที่สามารถใช้งานได้ฟรีและใช้ระบบอัตโนมัติในการจัดการใบรับรองความปลอดภัยสำหรับเว็บไซต์เข้ารหัส โดยเราจะใช้งานผ่าน client ที่มีให้ มีจุดมุ่งหมายเพื่อสาธารณประโยชน์ [5] ระบบของ Let's Encrypt ให้บริการโดย Internet Security Research Group (ISRG) กระบวนการขอใบรับรองจะจัดการผ่านโปรโตคอลที่เรียกว่า Automated Certificate Management Environment (ACME) [6] โดยโปรโตคอลนี้สร้างขึ้นมาเพื่อที่จะทำให้กระบวนการยืนยันโดเมน (Domain Validation) กระทำได้อย่างอัตโนมัติโดยไม่ต้องมีมนุษย์เข้าไปเกี่ยวข้องโดยสิ้นเชิง ผู้ดูแลระบบเครือข่ายต้องระบุอีเมลและโดเมนที่ต้องการลงไปใน ACME server เพื่อเป็นตัวรับรองเครือข่ายของตนเอง โดยผ่านการรับรองยืนยันโดเมน Domain Validation with Server Name Indication (DVSNI) หลังจากผ่านกระบวนการรับรองเสร็จแล้ว ACME server จะเชื่อมต่อเข้ามาและตรวจสอบใบรับรอง ถ้าถูกต้องกระบวนการยืนยันโดเมนก็จะเสร็จสมบูรณ์

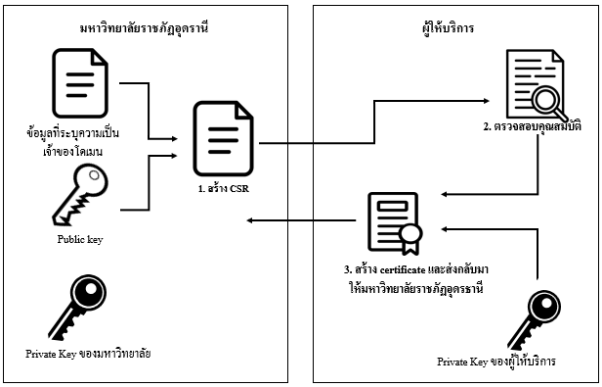
2.4 กระบวนการทำระบบ SSL มหาวิทยาลัยราชภัฏอุดรานี

มหาวิทยาลัยราชภัฏอุดรานี ได้จัดทำระบบ SSL/TLS certificates ที่รองรับความปลอดภัยทางอิเล็กทรอนิกส์ โดยเป็น SSL/TLS certificates ประเภท Wildcard SSL [7] ซึ่งรองรับทุกซับโดเมน ภายใต้โดเมนหลัก udru.ac.th ไม่จำกัดประเภท Web Server โดยมีกระบวนการดังนี้

2.4.1 สร้าง Certificate Signing Request (CSR) [8] โดยใช้ข้อมูลที่ระบุความเป็นเจ้าของโดเมน Public Key และ Private Key ส่งให้ผู้ให้บริการ

2.4.2 ผู้ให้บริการตรวจสอบความถูกต้อง CSR โดยมีการยืนยันความเป็นเจ้าของโดเมน

2.4.3 ผู้ให้บริการสร้าง SSL/TLS certificates ที่ระบุเป็นโดนเมนของมหาวิทยาลัยและส่งกลับกลับมาให้กับทางมหาวิทยาลัย ดังแสดงในรูปที่ 1



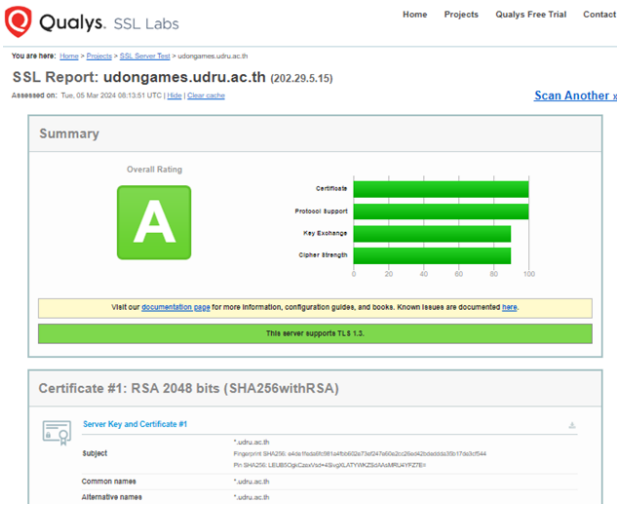
รูปที่ 1 กระบวนการสร้าง SSL/TLS certificates

เมื่อเว็บไซต์ได้ทำการติดตั้ง SSL/TLS certificates แล้ว จะทำการตั้งค่าที่เครื่องเซิร์ฟเวอร์ให้มีการบังคับใช้ SSL/TLS certificates ด้วยการ redirect http to https เพื่อความปลอดภัยเมื่อมีการเข้าเว็บไซต์ [9]

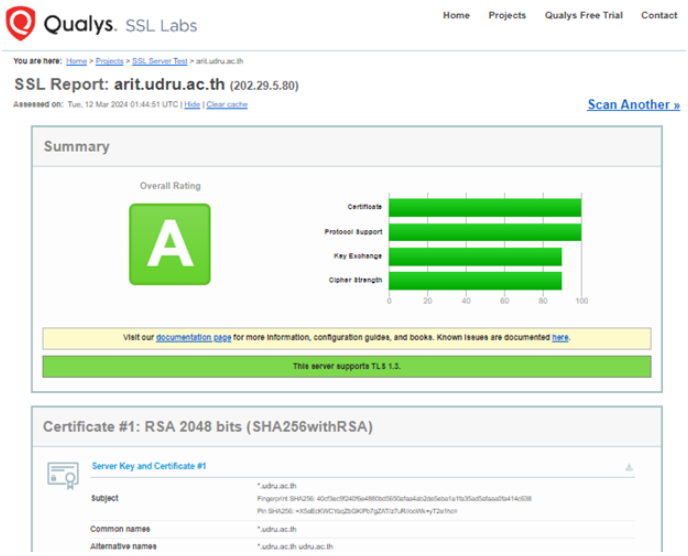
3. วิธีดำเนินการวิจัย

จากการทดลองใช้ SSL/TLS certificates ของ Let's Encrypt และแบบซื้อผ่านผู้ให้บริการ ผู้วิจัยได้แบ่งการทดลองออกเป็น 5 ด้าน ดังนี้

3.1 ในด้านความปลอดภัย จากการทดสอบความปลอดภัยของ SSL/TLS certificates ผ่านเว็บไซต์ SSL Labs (www.ssllabs.com) ซึ่งเป็นเว็บไซต์สำหรับทดสอบและประเมินความปลอดภัยของเว็บไซต์ที่ใช้ SSL/TLS พบว่า SSL/TLS certificates ทั้งแบบซื้อผ่านผู้บริการและของ Let's Encrypt จะให้ผลการทดสอบที่คล้ายคลึงกัน ซึ่งผลการทดสอบนอกจากจะขึ้นอยู่กับ SSL/TLS certificates แล้วยังขึ้นอยู่กับการกำหนดค่าความปลอดภัยในส่วนของ Server [10] อีกด้วย ผลการทดสอบเว็บไซต์ที่ติดตั้ง SSL/TLS certificates ของ Let's Encrypt ดังแสดงในรูปที่ 2 และรูปที่ 3



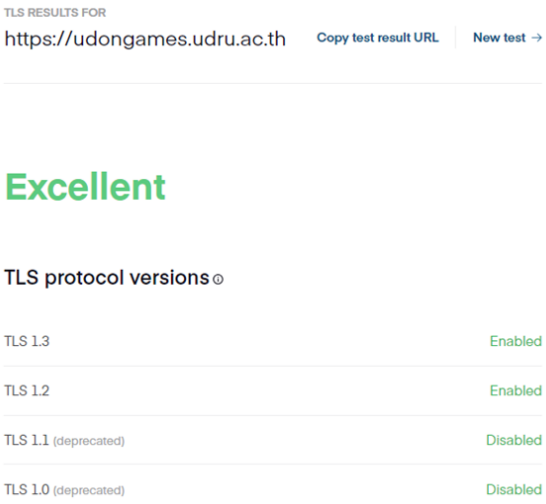
รูปที่ 2 ผลการทดสอบเว็บไซต์ที่ติดตั้ง SSL/TLS certificates ของ Let's Encrypt



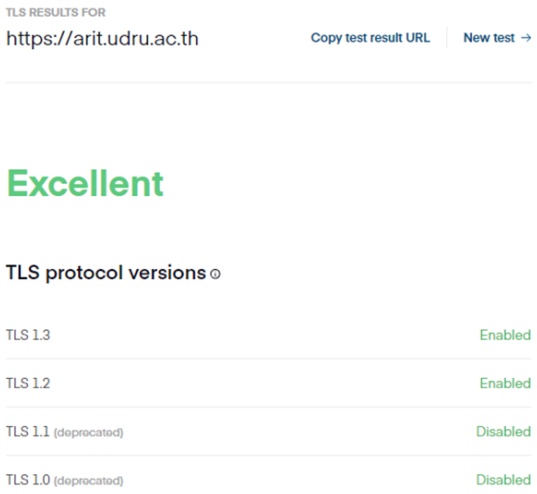
รูปที่ 3 ผลการทดสอบเว็บไซต์ที่ติดตั้ง SSL/TLS certificates ซื้อผ่านผู้บริการ

3.2 ในด้านค่าใช้จ่าย ค่าใช้จ่ายในการใช้บริการผ่านผู้บริการสำหรับ SSL/TLS certificates แบบ wildcard ที่รองรับทุกโดเมนของมหาวิทยาลัย (*.udru.ac.th) ค่าใช้จ่ายอยู่ที่ประมาณ 25,000 บาท/ปี ในขณะที่ SSL/TLS certificates ของ Let's Encrypt จะไม่มีค่าใช้จ่ายและสามารถใช้แบบ wildcard ที่รองรับทุกโดเมนของมหาวิทยาลัย (*.udru.ac.th) ได้เช่นกัน

3.3 ด้านการรองรับจากเว็บเบราว์เซอร์ ทั้ง SSL/TLS certificates แบบที่ซื้อผ่านผู้ให้บริการ และจาก Let's Encrypt สามารถรองรับเว็บเบราว์เซอร์ทุกชนิด จากการใช้ โพรโทคอล TLS เวอร์ชัน 1.3 เหมือนกัน ดังภาพ



รูปที่ 4 โพรโทคอล TLS เวอร์ชั่น 1.3 จากเว็บไซต์ที่ติดตั้ง SSL/TLS certificates ของ Let's Encrypt



รูปที่ 5 โพรโทคอล TLS เวอร์ชั่น 1.3 จากเว็บไซต์ที่ติดตั้ง SSL/TLS certificates ซื้อผ่านผู้บริการ

3.4 ด้านการสนับสนุนทางเทคนิค SSL/TLS certificates แบบที่ซื้อผ่านผู้ให้บริการ จะสามารถให้ผู้บริการเข้ามาดูแลและสนับสนุนทางเทคนิคได้ แต่ส่วนของ SSL/TLS certificates แบบ

Let's Encrypt จะไม่มีการให้บริการสนับสนุนทางเทคนิค มหาวิทยาลัยราชภัฏอุดรธานี มีผู้ดูแลระบบเครือข่าย ที่สามารถเข้าอบรมเรียนรู้เกี่ยวกับเทคนิคด้านเทคนิคการแก้ไขปัญหานี้ได้

3.5 ในด้านระยะเวลาการใช้งาน ระยะเวลาการใช้งานของ SSL/TLS certificates ที่ซื้อผ่านผู้ให้บริการจะมีอายุการใช้งาน 1 ปี ในขณะที่ SSL/TLS certificates จาก Let's Encrypt จะมีอายุการใช้งาน 90 วัน ซึ่งจะมีการต่ออายุอัตโนมัติโดยระบบเองจนกว่าจะถึง 1 ปี และเมื่อครบ 1 ปี ผู้ดูแลระบบเครือข่ายสามารถต่ออายุการใช้งานของ SSL/TLS certificates ได้ด้วยตนเอง

จาก 5 ด้านที่ ได้ทำการวิเคราะห์และเปรียบเทียบระหว่าง SSL/TLS certificates จาก ผู้ให้บริการและ จาก Let's Encrypt สามารถสรุปเป็นตารางได้ดังนี้

ตารางที่ 1 ตารางเปรียบเทียบ SSL/TLS certificates จาก ผู้ให้บริการและ จาก Let's Encrypt

ด้านที่วิเคราะห์	จากผู้ให้บริการ	Let's Encrypt
ความปลอดภัย	เทียบเคียงกัน	
ค่าใช้จ่าย	25000 บาท/ปี	0 บาท/ปี
การรับรองจากเว็บบราวเซอร์	ได้เหมือนกัน	
การสนับสนุน	ผู้ให้บริการ	ผู้ดูแลระบบเครือข่าย
ระยะเวลาในการใช้งาน	1 ปี ซื้อจากผู้ให้บริการ	1 ปี และสามารถต่ออายุของปีถัดไปโดยผู้ดูแลระบบเครือข่ายได้

4. สรุปผลและข้อเสนอแนะ

จากผลการทดสอบการใช้งาน SSL/TLS certificates ของ Let's Encrypt แสดงให้เห็นว่าสามารถใช้งานทดแทนการใช้ SSL/TLS certificates แบบซื้อจากผู้ให้บริการ ที่มีปลอดภัยที่เทียบเคียงกันได้ สามารถรองรับเว็บบราวเซอร์ได้เหมือนกัน SSL/TLS นอกจากนี้ certificates ของ Let's Encrypt สามารถจัดการ สามารถต่ออายุในปีถัดไปและดูแลโดยตรงจากผู้ดูแลระบบเครือข่าย โดยไม่มีค่าใช้จ่ายในการใช้ SSL/TLS certificates ดังนั้นการใช้ SSL/TLS certificates ของ Let's Encrypt สามารถนำไปใช้ได้จริง และช่วยลดค่าใช้จ่ายในการรักษาความปลอดภัยของเว็บไซต์ในมหาวิทยาลัยราชภัฏอุดรธานีได้ถึง ปีละ 25,000 บาท

เอกสารอ้างอิง

[1] Dierks, T. and Allen, C. (1999). **The TLS Protocol Version 1.0**. Retrieved from https://datatracker.ietf.org/doc/html/rfc2246.

[2] Rescorla, E. (2018). **The Transport Layer Security (TLS) Protocol Version1.3**. Retrieved from https://datatracker.ietf.org /doc/html/rfc8446.

[3] Rescorla, E. (2000). **HTTP Over TLS** Retrieved from https://datatracker.ietf.org/doc/html/rfc2818.

[4] Fielding, R. (2022). **HTTP/1 . 1 : IETF.** Retrieved from https://datatracker.ietf.org/doc/html/rfc9112.

[5] Aas, J., Barnes, R., Case, B., Durumeric, Z., Eckersley, P., Flores-López, A., Alex Halderman, J., Hoffman-Andrews, J., Kasten, J., Rescorla, E., Schoen, S. and Warren, B. (2019). Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web. **In Proceedings of ACM SIGSAC Conference on Computer and Communications Security**, pp.2473–2487. London, United Kingdom.

[6] Barnes R. (2019). **Automatic Certificate Management Environment (ACME)**. Retrieved from https://datatracker.ietf.org/ doc/html/rfc8555.

[7] Lewis, E. (2006). **The Role of Wildcards in the Domain Name System**. Retrieved from https://datatracker.ietf.org/doc/html /rfc4592.

[8] Kaliski, B. (1998). **PKCS #10: Certification Request Syntax Version 1.5**. Retrieved from https://datatracker.ietf.org/doc/html/ rfc2314.

[9] Jackson, C. and Barth, A. (2008). ForceHTTPS: Protecting High-security Web Sites from Network Attacks. **In Proceedings of the 17th International World Wide Web Conference**, pp. 525-534. United States.

[10] RistiC, V. (2024). **SSL/TLS Deployment Best Practices. SSL Labs.** Retrieved from https://www.ssllabs.com/projects/best-practices.