ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard for Electronic Transactions

ขมธอ. [x-xxxx]

ว่าด้วยการประทับเวลาอิเล็กทรอนิกส์

ELECTRONIC TIME-STAMPING

เวอร์ชัน 0.2

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.030

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการประทับเวลาอิเล็กทรอนิกส์

ขมธอ. [x-xxxx]

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 20-22
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

ประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ กรุณาเลือกวันที่ประกาศ

คณะทำงานจัดทำร่างข้อเสนอแนะมาตรฐานเกี่ยวกับธุรกิจบริการ
ด้านการทำธุรกรรมทางอิเล็กทรอนิกส์

ที่ปรึกษาคณะทำงาน

นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ประธานคณะทำงาน

นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ทำงาน

นางสาวสำรวย นุ่มศรี	กรมศุลกากร
นายกำชัย จัตตานนท์	
นายนิรันดร์ ประจวบเหมาะ	กรมสรรพากร
นางสุภิดา บรรเทาทุกข์	
นายคงฤทธิ์ จันทริก	สภาผู้ส่งสินค้าทางเรือแห่งประเทศไทย
นายภาวุธ พงษ์วิทยภานุ	สมาคมผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ไทย
นายธานินทร์ ตันกิติบุตร	สมาคมผู้ให้บริการอินเทอร์เน็ตไทย
นายวรพจน์ ธาราศิริสกุล	สมาคมฟินเทคประเทศไทย
นายปกรณ์ ลี้สกุล	สมาคมอุตสาหกรรมซอฟต์แวร์ไทย
นางสาวขนิษฐ์ ผาทอง	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายพงษ์พันธ์ ศรีปาน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ทำงานและเลขานุการ

นายณัฐฑพัฒน์ โรจนศุภมิตร	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ช่วยเลขานุการ

นายวีรศักดิ์ ดีอ่ำ	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

วิเคราะห์และจัดทำข้อเสนอแนะมาตรฐานฯ
ว่าด้วยการประทับเวลาอิเล็กทรอนิกส์

นายปกรณ์ ลี้สกุล	สมาคมไทยบล็อกเชน
นายณัฐวุฒิ กองสุวรรณ	สมาคมไทยบล็อกเชน
นายสัมโมทิก สวิชญาน	สมาคมไทยบล็อกเชน
นางสาวนันท์นภัส ทรงมณี	สมาคมไทยบล็อกเชน
นางสาววราภรณ์ หลีสกุล	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายณัฐพัฒน์ โรจนศุภมิตร	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการประทับเวลาอิเล็กทรอนิกส์ฉบับนี้ จัดทำขึ้นเพื่ออธิบายคำศัพท์ กระบวนการ และกรณีการใช้งานที่เกี่ยวข้องกับการประทับเวลาอิเล็กทรอนิกส์ (electronic time-stamping) เพื่อให้ผู้ที่เกี่ยวข้องกับการประทับเวลาอิเล็กทรอนิกส์มีความเข้าใจตรงกัน รวมทั้งกำหนดแนวทางในการจัดทำแนวนโยบายและแนวปฏิบัติของผู้ให้บริการประทับเวลา (time-stamping authority: TSA) เพื่อให้การให้บริการประทับเวลาของ TSA ในประเทศไทยมีความน่าเชื่อถือและสอดคล้องตามมาตรฐานสากล

โดยมีการนำเสนอและรับฟังความคิดเห็นเป็นการทั่วไป ตลอดจนพิจารณาข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วนยิ่งขึ้น รวมทั้งให้สามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการประทับเวลาอิเล็กทรอนิกส์ฉบับนี้ จัดทำขึ้นโดยสมาคมไทยบล็อกเชน ร่วมกับสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 20-22 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200
อีเมล: estandard.center@etda.or.th
เว็บไซต์: www.etda.or.th

คำนำ

ด้วยปัจจุบันการประกอบธุรกิจของภาคเอกชนและการให้บริการประชาชนของหน่วยงานภาครัฐ ได้ปรับเปลี่ยนแนวทางการทำธุรกรรมโดยอาศัยเทคโนโลยีสารสนเทศมากขึ้น เช่น การใช้งานเอกสารอิเล็กทรอนิกส์ การลงลายมือชื่ออิเล็กทรอนิกส์ รวมทั้งการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งจะส่งผลให้การทำธุรกรรมทางอิเล็กทรอนิกส์เป็นกลไกสำคัญในการขับเคลื่อนเศรษฐกิจในยุคดิจิทัล

การประทับเวลาอิเล็กทรอนิกส์ (electronic time-stamping) เป็นหนึ่งในกระบวนการเสริมสร้างความน่าเชื่อถือในระบบข้อมูลอิเล็กทรอนิกส์ ด้วยการเชื่อมโยงค่าเวลาและวันที่กับข้อมูลอิเล็กทรอนิกส์ เพื่อให้มีหลักฐานว่าข้อมูลอิเล็กทรอนิกส์นั้นมีอยู่จริง ณ เวลาดังกล่าว ทั้งนี้ การประทับเวลาอิเล็กทรอนิกส์สามารถนำไปใช้ประโยชน์ได้หลายด้าน เช่น การใช้งานการประทับเวลาอิเล็กทรอนิกส์ร่วมกับลายมือชื่ออิเล็กทรอนิกส์ การระบุเวลาที่น่าเชื่อถือของการออกเอกสารหรือการลงลายมือชื่อ และการเก็บรักษาข้อมูลและลายมือชื่อในระยะยาว เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและความน่าเชื่อถือ

ด้วยเหตุนี้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำข้อเสนอแนะมาตรฐานฯ ว่าด้วยการประทับเวลาอิเล็กทรอนิกส์ เพื่ออธิบายคำศัพท์ กระบวนการ และกรณีการใช้งานที่เกี่ยวข้องกับการประทับเวลาอิเล็กทรอนิกส์ เพื่อให้ผู้ที่เกี่ยวข้องกับการประทับเวลาอิเล็กทรอนิกส์มีความเข้าใจตรงกัน รวมทั้งกำหนดแนวทางในการจัดทำแนวนโยบายและแนวปฏิบัติของผู้ให้บริการประทับเวลา (time-stamping authority: TSA) เพื่อให้การให้บริการประทับเวลาของ TSA ในประเทศไทยมีความน่าเชื่อถือและสอดคล้องตามมาตรฐานสากล

สารบัญ

สารบัญรูป

หน้า

สารบัญตาราง

หน้า

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยการประทับเวลาอิเล็กทรอนิกส์

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้อธิบายคำศัพท์ กระบวนการ และกรณีการใช้งานที่เกี่ยวข้องกับการประทับเวลาอิเล็กทรอนิกส์ (electronic time-stamping) เพื่อให้ผู้ที่เกี่ยวข้องกับการประทับเวลาอิเล็กทรอนิกส์มีความเข้าใจตรงกัน รวมทั้งกำหนดแนวทางในการจัดทำแนวนโยบายและแนวปฏิบัติของผู้ให้บริการประทับเวลา (time-stamping authority: TSA) เพื่อให้การให้บริการประทับเวลาของ TSA ในประเทศไทยมีความน่าเชื่อถือและสอดคล้องตามมาตรฐานสากล

2. บทนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 โทเคนประทับเวลา (time-stamp token) หรือ ตราประทับเวลา (time stamp) หมายถึง ข้อมูลที่เชื่อมโยงค่าเวลาและวันที่กับข้อมูลอิเล็กทรอนิกส์ เพื่อให้มีหลักฐานว่าข้อมูลอิเล็กทรอนิกส์นั้นมีอยู่จริง ณ เวลาดังกล่าว

2.2 บริการประทับเวลา (time-stamping service) หมายถึง บริการที่ออกโทเคนประทับเวลา เพื่อให้มีหลักฐานว่าข้อมูลอิเล็กทรอนิกส์มีอยู่จริง ณ เวลาใดเวลาหนึ่ง

2.3 ผู้ให้บริการประทับเวลา (time-stamping authority: TSA) หมายถึง หน่วยงานที่ให้บริการประทับเวลาด้วยการออกโทเคนประทับเวลา

2.4 ผู้ขอประทับเวลา (time-stamp requester) หมายถึง บุคคลที่มีข้อมูลอิเล็กทรอนิกส์ที่ต้องการนำไปประทับเวลา

หมายเหตุ: ผู้ขอประทับเวลาสามารถเป็นบุคคลที่สามที่เชื่อถือได้ ซึ่งรวมถึง TSA

2.5 ผู้ตรวจสอบประทับเวลา (time-stamp verifier) หมายถึง บุคคลที่ต้องการตรวจสอบว่าข้อมูลอิเล็กทรอนิกส์มีการประทับเวลาที่ถูกต้องหรือไม่

หมายเหตุ: กระบวนการตรวจสอบสามารถทำได้โดยผู้ตรวจสอบประทับเวลาเองหรือบุคคลที่สามที่เชื่อถือได้

2.6 มาตรเวลาร่วมสากล (coordinated universal time: UTC) หมายถึง มาตรเวลา (time scale) ที่ดูแลโดยสำนักงานชั่งตวงวัดระหว่างประเทศ (Bureau International des Poids et Mesures: BIPM) และใช้เป็นรากฐานของการเผยแพร่ความถี่และสัญญาณเวลาที่เป็นมาตรฐานร่วมกัน

2.7 UTC(k) หมายถึง มาตรเวลา (time scale) ที่คำนวณโดยห้องปฏิบัติการ “k” และมีการเทียบเวลากับมาตรเวลาร่วมสากล (UTC) เพื่อให้มีความสอดคล้องกันภายใน ±100 ns

หมายเหตุ: UTC(NIMT) คือ มาตรเวลาของประเทศไทยที่ดูแลโดยสถาบันมาตรวิทยาแห่งชาติ (National Institute of Metrology (Thailand): NIMT)

2.8 ศูนย์เวลา (timing centre) หมายถึง หน่วยงานที่มีช่องทางในการเผยแพร่เวลา UTC(k) ไปยัง TSA ตามค่าความแม่นยำที่กำหนด

2.9 ผู้ประเมินเวลา (time assessment authority: TAA) หมายถึง หน่วยงานที่ตรวจสอบเวลาของนาฬิกาของ TSA และอาจเผยแพร่เวลาไปยัง TSA ด้วย

2.10 ลายมือชื่ออิเล็กทรอนิกส์ (electronic signature) หมายถึง อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น [1]

2.11 ลายมือชื่อดิจิทัล (digital signature) หมายถึง ลายมือชื่ออิเล็กทรอนิกส์ที่ได้จากกระบวนการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ ซึ่งช่วยให้สามารถยืนยันตัวเจ้าของลายมือชื่อ และตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้ รวมถึงการทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเองลงลายมือชื่อได้ [1]

2.12 กุญแจส่วนตัว (private key) หมายถึง กุญแจที่ใช้สร้างลายมือชื่อดิจิทัล และสามารถนำไปใช้ในการถอดรหัสลับเมื่อมีการเข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ [2]

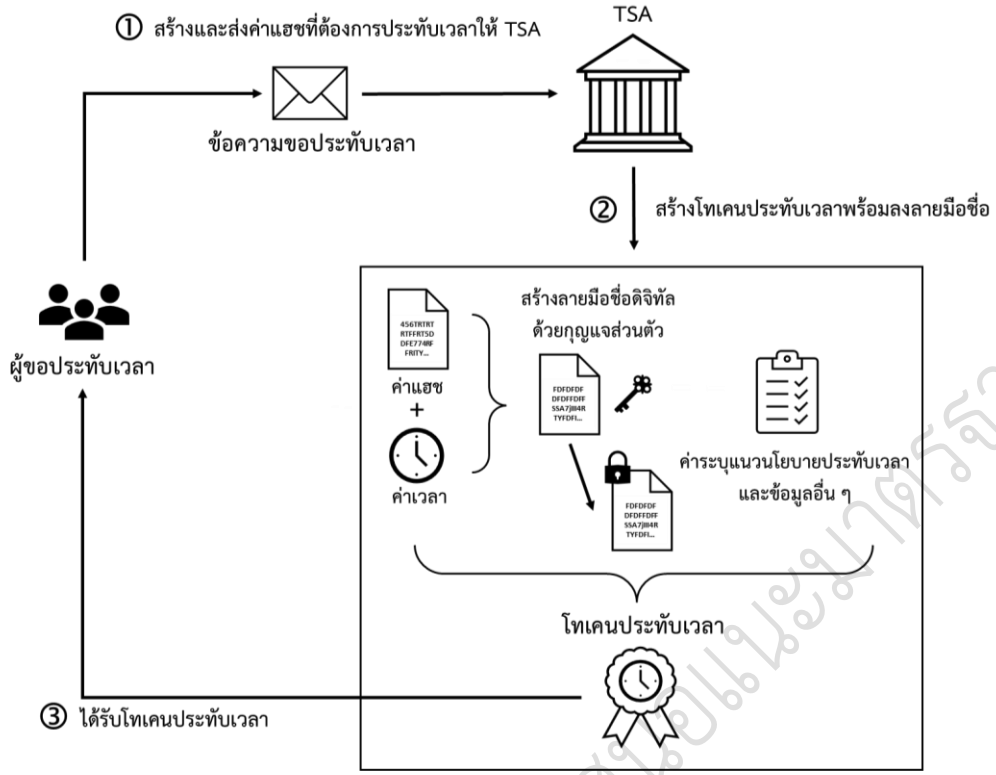
2.13 กุญแจสาธารณะ (public key) หมายถึง กุญแจที่ใช้ตรวจสอบลายมือชื่อดิจิทัล และสามารถนำไปใช้เข้ารหัสลับข้อมูลอิเล็กทรอนิกส์ เพื่อมิให้สามารถเข้าใจความหมายของข้อมูลอิเล็กทรอนิกส์ที่มีการเข้ารหัสลับนั้นได้ เพื่อประโยชน์ในการรักษาความลับของข้อมูลอิเล็กทรอนิกส์นั้น [2]

3. ภาพรวมของการประทับเวลาอิเล็กทรอนิกส์

การประทับเวลาอิเล็กทรอนิกส์ เป็นหนึ่งในกระบวนการเสริมสร้างความน่าเชื่อถือในระบบข้อมูลอิเล็กทรอนิกส์ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและความน่าเชื่อถือ โดยผู้ให้บริการประทับเวลา (time-stamping authority: TSA) ทำหน้าที่เป็นบุคคลที่สามที่เชื่อถือได้ในการให้บริการประทับเวลาด้วยการออกโทเคนประทับเวลา (time-stamp token) ที่เชื่อมโยงค่าเวลากับข้อมูลอิเล็กทรอนิกส์ในลักษณะที่ไม่สามารถปลอมแปลงได้ เพื่อให้มีหลักฐานว่าข้อมูลอิเล็กทรอนิกส์นั้นมีอยู่จริง ณ เวลาใดเวลาหนึ่ง นอกจากนี้ ค่าเวลาที่อยู่ในโทเคนประทับเวลาจะต้องมีการประสานเวลากับมาตรเวลาร่วมสากล (coordinated universal time: UTC) เพื่อให้มั่นใจว่าค่าเวลาที่อยู่ในโทเคนประทับเวลามีความแม่นยำ

3.1 การสร้างโทเคนประทับเวลา

กระบวนการประทับเวลาหรือกระบวนการสร้างโทเคนประทับเวลา สามารถแสดงเป็นแผนภาพตามรูปที่ 1



รูปที่ 1 การสร้างโทเคนประทับเวลา

(1) ผู้ขอประทับเวลาสร้างค่าแฮช (hash value)[1] สำหรับข้อมูลอิเล็กทรอนิกส์ที่จะประทับเวลา และส่งค่าแฮชไปยัง TSA ด้วยข้อความขอประทับเวลา (time-stamp request message)

(2) TSA เชื่อมโยงค่าแฮชและข้อความขอประทับเวลาเข้ากับค่าเวลาปัจจุบัน (current time value) และสร้างเป็นโทเคนประทับเวลา (time-stamp token) ส่งกลับไปยังผู้ขอประทับเวลา ทั้งนี้ TSA ต้องสร้างลายมือชื่อดิจิทัลต่อโทเคนประทับเวลาด้วยการใช้กุญแจส่วนตัว[2] โดยมีใบรับรองกุญแจสาธารณะ (public key certificate) ที่ระบุว่าการใช้งานกุญแจนั้นมีวัตถุประสงค์เพื่อการประทับเวลาโดยเฉพาะ

(3) ผู้ขอประทับเวลาได้รับโทเคนประทับเวลาที่มีลายมือชื่อดิจิทัลของ TSA และสามารถนำไปประกอบกับข้อมูลอิเล็กทรอนิกส์ที่เกี่ยวข้อง

---

[1] ค่าแฮช (hash value) เป็นผลลัพธ์ของฟังก์ชันแฮช (hash function) ซึ่งหมายถึง ฟังก์ชันทางคณิตศาสตร์ที่ประมวลผลข้อมูลตั้งต้นแล้วให้ผลลัพธ์ที่มีความยาวคงที่ โดยไม่สามารถนำผลลัพธ์มาคำนวณกลับเป็นข้อมูลตั้งต้นได้ และไม่สามารถหาข้อมูลตั้งต้นที่แตกต่างกันซึ่งให้ผลลัพธ์ที่เหมือนกันได้ ทั้งนี้ รายละเอียดของฟังก์ชันแฮชจะระบุไว้ในอนุกรมมาตรฐาน ISO/IEC 10118

[2] TSA อาจจัดการหน่วยประทับเวลา (time-stamping unit: TSU) หลายหน่วยเพื่อวัตถุประสงค์ของการให้บริการที่ระดับแตกต่างกันหรือการกระจายภาระงาน (load balancing) โดย TSU แต่ละหน่วยจะมีกุญแจส่วนตัวที่แตกต่างกันสำหรับใช้สร้างลายมือชื่อดิจิทัลต่อโทเคนประทับเวลา

3.2 โทเคนประทับเวลา

โทเคนประทับเวลา (time-stamp token) เป็นข้อมูลที่เชื่อมโยงค่าเวลาและวันที่กับข้อมูลอิเล็กทรอนิกส์ เพื่อให้มีหลักฐานว่าข้อมูลอิเล็กทรอนิกส์นั้นมีอยู่จริง ณ เวลาดังกล่าว ทั้งนี้ โทเคนประทับเวลาจะประกอบด้วยข้อมูลต่าง ๆ ดังนี้

- ค่าแฮชของข้อมูลที่จะประทับเวลา
- ค่าเวลา ณ เวลาใดเวลาหนึ่ง
- ค่าระบุแนวนโยบายการประทับเวลา (time-stamp policy) ที่ใช้ในการสร้างโทเคนประทับเวลา

รวมถึงข้อมูลเพิ่มเติมตามที่ระบุไว้ใน RFC 3161 [3] ซึ่งอาจเป็นประโยชน์ต่อการให้บริการประทับเวลา เช่น

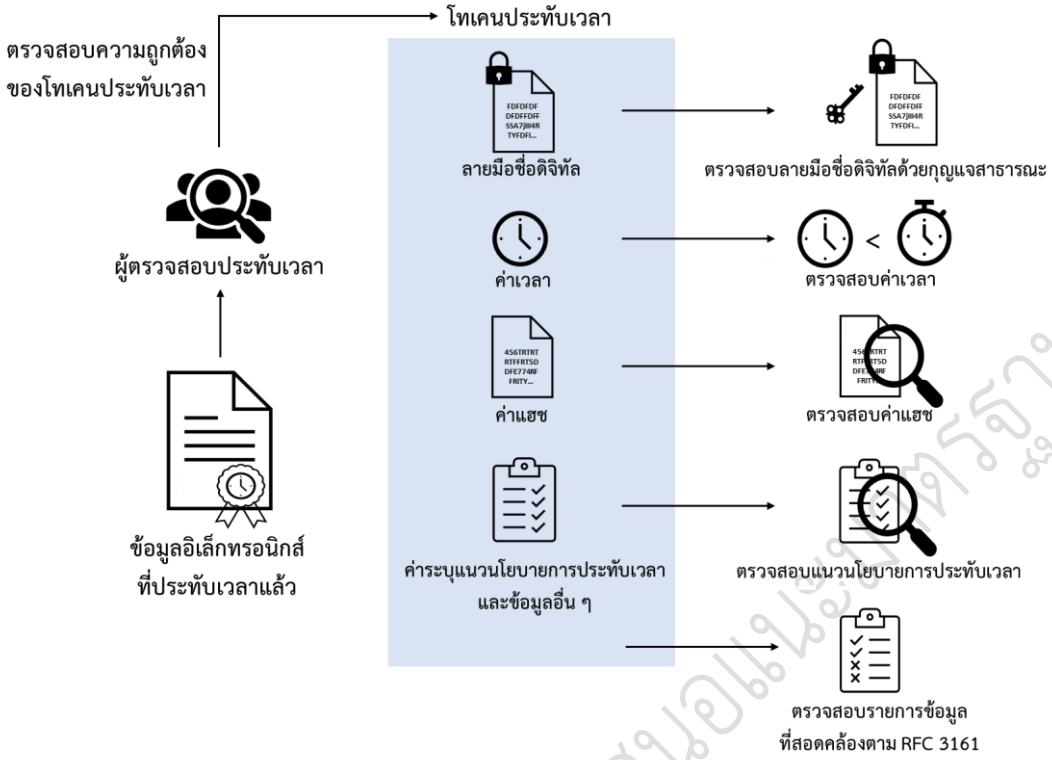
- ค่าระบุตัวตนของ TSA ที่ให้บริการ
- ค่าความแม่นยำของค่าเวลา
- หมายเลขลำดับของโทเคนประทับเวลา
- หมายเลขคำขอประทับเวลา

3.3 การตรวจสอบโทเคนประทับเวลา

เมื่อได้รับข้อมูลอิเล็กทรอนิกส์ที่ประทับเวลาแล้ว ผู้ตรวจสอบประทับเวลาสามารถตรวจสอบความถูกต้องของโทเคนประทับเวลาด้วยตนเองหรือมอบหมายให้บุคคลที่สามที่เชื่อถือได้ดำเนินการแทน โดยให้ดำเนินการตรวจสอบดังนี้

- ตรวจสอบลายมือชื่อดิจิทัลของโทเคนประทับเวลาด้วยกุญแจสาธารณะของ TSA รวมถึงตรวจสอบสถานะของใบรับรองกุญแจสาธารณะของ TSA
- ตรวจสอบว่าโทเคนประทับเวลามีรายการข้อมูล (data fields) ที่สอดคล้องตาม RFC 3161
- ตรวจสอบว่าค่าเวลาที่อยู่ในโทเคนประทับเวลาเป็นเวลาก่อนหน้า ค่าเวลาในขณะที่ตรวจสอบโทเคนประทับเวลา
- ตรวจสอบว่าค่าแฮชที่อยู่ในโทเคนประทับเวลาตรงกับค่าแฮชของข้อมูลอิเล็กทรอนิกส์ที่ต้องการตรวจสอบ โดยใช้ฟังก์ชันแฮชแบบเดียวกันกับฟังก์ชันแฮชที่ใช้ในการสร้างโทเคนประทับเวลา
- ตรวจสอบว่าแนวนโยบายการประทับเวลาที่ใช้ในการสร้างโทเคนประทับเวลามีความเหมาะสมกับวัตถุประสงค์การใช้งานของผู้ตรวจสอบประทับเวลา

หากสอดคล้องตามเงื่อนไขข้างต้นทั้งหมด จะถือว่าโทเคนประทับเวลามีความถูกต้อง ณ เวลาที่ทำการตรวจสอบโทเคนประทับเวลา โดยการตรวจสอบโทเคนประทับเวลาสามารถแสดงเป็นแผนภาพตามรูปที่ 2



รูปที่ 2 การตรวจสอบโทเคนประทับเวลา

3.3.1 ข้อพิจารณาด้านความมั่นคงปลอดภัย

ในการตรวจสอบโทเคนประทับเวลา ผู้ตรวจสอบประทับเวลาจำเป็นต้องตรวจสอบให้มั่นใจว่าใบรับรองกุญแจสาธารณะของ TSA มีความน่าเชื่อถือและยังไม่ถูกเพิกถอน ซึ่งหมายความว่า ความมั่นคงปลอดภัยของโทเคนประทับเวลาจะขึ้นอยู่กับความมั่นคงปลอดภัยของผู้ให้บริการออกใบรับรอง (certification authority: CA) ในการออกใบรับรองกุญแจสาธารณะให้กับ TSA และการให้ข้อมูลสถานะการเพิกถอนใบรับรองนั้นอย่างถูกต้องและเป็นปัจจุบัน

นอกจากนี้ ถึงแม้ว่าโทเคนประทับเวลาจะได้รับการตรวจสอบว่ามีความถูกต้อง ณ เวลาที่ตรวจสอบโทเคนประทับเวลา ก็ไม่ได้หมายความว่า โทเคนประทับเวลานั้นจะมีความถูกต้องหรือยังคงใช้ได้ในภายหลัง ดังนั้น ในการตรวจสอบโทเคนประทับเวลาในช่วงเวลาที่ใบรับรองกุญแจสาธารณะของ TSA ยังไม่หมดอายุ ก็ยังจำเป็นต้องมีการตรวจสอบข้อมูลสถานการณ์เพิกถอนใบรับรองด้วยทุกครั้ง เนื่องจากในกรณีที่กุญแจส่วนตัวของ TSA ถูกล่วงรู้โดยผู้ที่ไม่ได้รับอนุญาต โทเคนประทับเวลาทั้งหมดที่ถูกสร้างโดยกุญแจส่วนตัวของ TSA ดังกล่าวภายหลังจากการเพิกถอนใบรับรอง จะถือว่าไม่สามารถใช้งานได้

3.4 การต่ออายุโทเคนประทับเวลา

TSA อาจดำเนินการต่ออายุโทเคนประทับเวลา โดยการนำข้อมูลอิเล็กทรอนิกส์ที่ประทับเวลาแล้วมาประทับเวลาอีกครั้งในภายหลังได้ เนื่องจากอาจมีความจำเป็นด้วยเหตุผล เช่น

- กลไกที่ใช้เชื่อมโยงค่าเวลากับข้อมูลกำลังจะสิ้นสุดวงจรการใช้งาน (operational life cycle) เช่น กุณแจส่วนตัวหรือใบรับรองกุญแจสาธารณะของ TSA กำลังจะหมดอายุ

- ฟังก์ชันการเข้ารหัสลับ (cryptographic function) ที่ใช้เชื่อมโยงค่าเวลาเข้ากับข้อมูลกำลังจะไม่น่าเชื่อถืออีกต่อไปหรือมีหลักฐานว่าจะพบช่องโหว่ในระยะเวลาอันใกล้ เช่น ฟังก์ชันแฮชกำลังจะถูกทำลายโดยการโจมตีรูปแบบใหม่หรือพลังในการประมวลผลที่มีอยู่
- TSA ที่เป็นผู้ออกโทเคนประทับเวลากำลังจะยุติการให้บริการประทับเวลา
- แนวนโยบายการประทับเวลาระบุจุดเวลาที่โทเคนประทับเวลาจะหมดอายุ

ในกรณีเช่นนี้ โทเคนประทับเวลาอันเดิม (ซึ่งมีข้อมูลอิเล็กทรอนิกส์ที่ประทับเวลาไว้แล้วก่อนหน้า) จะถูกรวมเป็นข้อมูลสำหรับการสร้างโทเคนประทับเวลาอันใหม่ โดยโทเคนประทับเวลาอันใหม่จะเป็นการเชื่อมโยงค่าเวลาใหม่ (ค่าเวลาปัจจุบัน) กับข้อมูลอิเล็กทรอนิกส์เดิมและโทเคนประทับเวลาอันเดิม เพื่อให้ช่วงเวลาใช้งานได้ (validity period) ของโทเคนประทับเวลาอันเดิม (t_0) ถูกขยายออกไปให้ครอบคลุมถึงช่วงเวลาของโทเคนประทับเวลาอันใหม่ (t_1) นอกจากนี้ การต่ออายุโทเคนประทับเวลาอาจมีการสร้างโทเคนประทับเวลาอันใหม่ต่อกันหลายครั้ง เพื่อขยายช่วงเวลาใช้งานได้ของโทเคนประทับเวลาอันเดิมออกไปเรื่อย ๆ ($t_0 < t_1 < t_2 < \ldots < t_n$) ทั้งนี้ การสร้างโทเคนประทับเวลาอันใหม่ในแต่ละครั้งต้องเกิดขึ้นก่อนที่โทเคนประทับเวลาอันก่อนหน้าจะหมดอายุ

ในการตรวจสอบโทเคนประทับเวลาที่มีการต่ออายุหลายครั้ง ผู้ตรวจสอบประทับเวลาจะตรวจสอบว่าโทเคนประทับเวลาอันแรก (สร้าง ณ เวลา t_0) ต้องมีความถูกต้อง ณ เวลาที่สร้างโทเคนประทับเวลาอันที่สอง (t_1) และจะตรวจสอบโทเคนประทับเวลาทุกอันในลักษณะเดียวกัน กล่าวคือ โทเคนประทับเวลาแต่ละอันต้องมีความถูกต้อง ณ เวลาที่สร้างโทเคนประทับเวลาอันถัดไป และสุดท้าย โทเคนประทับเวลาอันล่าสุด (สร้าง ณ เวลา t_n) ต้องมีความถูกต้อง ณ เวลาปัจจุบันที่ทำการตรวจสอบ ทั้งนี้ เมื่อตรวจสอบโทเคนประทับเวลาทุกอันว่ามีความถูกต้องแล้ว ผู้ตรวจสอบประทับเวลาจึงจะสามารถสรุปได้ว่าข้อมูลอิเล็กทรอนิกส์ที่ประทับเวลาแล้วนั้น มีอยู่จริง ณ เวลาที่ทำการประทับเวลาครั้งแรก

3.5 การตรวจสอบย้อนกลับของเวลา

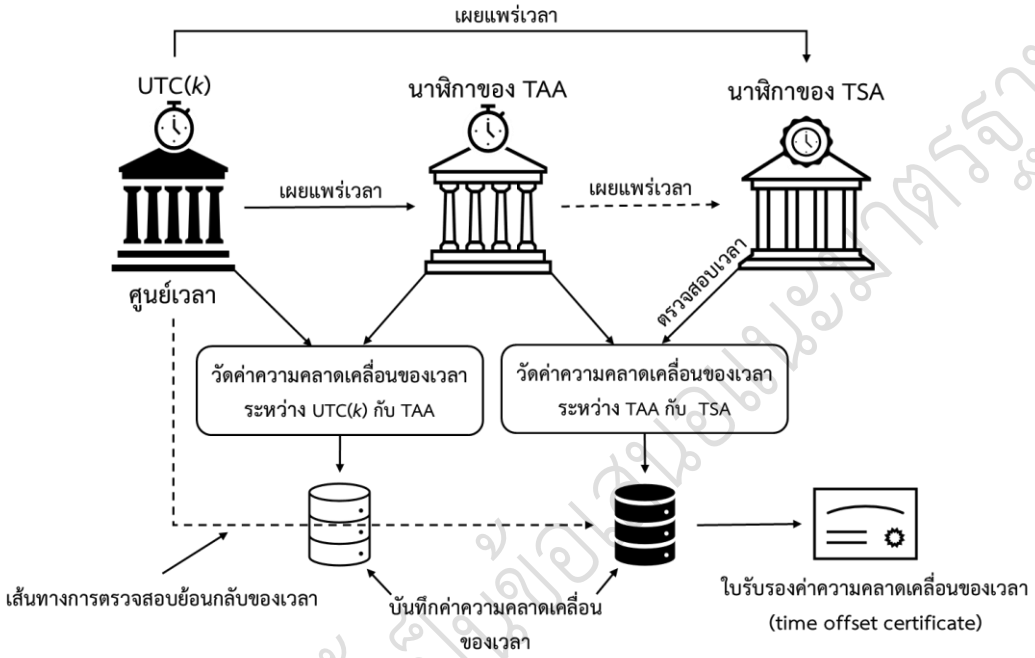
ในการให้บริการประทับเวลา นาฬิกาของ TSA ที่ใช้สร้างโทเคนประทับเวลาต้องมีการประสานเวลาให้สอดคล้องกันกับ UTC(k) ซึ่งเป็นมาตรเวลาที่คำนวณโดยห้องปฏิบัติการ “k” และเทียบเวลากับมาตรเวลาร่วมสากล (UTC) เพื่อให้ค่าเวลาที่อยู่ในโทเคนประทับเวลามีความน่าเชื่อถือ ทั้งนี้ UTC(k) ของประเทศไทยจะเป็น UTC(NIMT) ซึ่งหมายถึง มาตรเวลาที่คำนวณโดยสถาบันมาตรวิทยาแห่งชาติ (National Institute of Metrology (Thailand): NIMT)

ผู้ประเมินเวลา (time assessment authority: TAA) เป็นหน่วยงานที่ตรวจสอบเวลาของนาฬิกาของ TSA หรือเวลาอ้างอิงของ TSA ว่าสามารถตรวจสอบย้อนกลับ (time traceability) ไปยังมาตรเวลาของ UTC(k) ที่เผยแพร่จากศูนย์เวลา (time centre) ได้ โดย TAA จะออกใบรับรองค่าความคลาดเคลื่อนของเวลา (time offset certificate) ให้กับ TSA เพื่อยืนยันว่านาฬิกาของ TSA สามารถตรวจสอบย้อนกลับไปยัง UTC(k) ได้ภายในค่าความแม่นยำที่กำหนด

ทั้งนี้ TAA จะประสานเวลาของนาฬิกาของตนเองให้สอดคล้องกับ UTC(k) ที่เผยแพร่จากศูนย์เวลา และวัดค่าความคลาดเคลื่อนของเวลา (time offset) ระหว่าง UTC(k) กับนาฬิกาของ TAA และค่าความคลาดเคลื่อนของเวลาระหว่างนาฬิกาของ TAA กับนาฬิกาของ TSA เป็นระยะ ๆ จากนั้น TAA จะบันทึกค่าความคลาดเคลื่อนของเวลาที่วัดได้ ออกใบรับรองค่าความคลาดเคลื่อนของเวลาให้กับ TSA ตามช่วงเวลาที่

เหมาะสม และแจ้งให้ TSA ทราบเกี่ยวกับการสูญเสียความแม่นยำของเวลา หาก TAA ตรวจพบว่านาฬิกาของ TSA มีความคลาดเคลื่อนมากเกินไปจากค่าความแม่นยำที่กำหนด โดยการตรวจสอบย้อนกลับของเวลาสามารถแสดงเป็นแผนภาพตามรูปที่ 3

รายละเอียดเกี่ยวกับข้อกำหนดของ TAA และการตรวจสอบย้อนกลับของเวลา ให้เป็นไปตามมาตรฐาน ISO/IEC 18014-4 [4]



รูปที่ 3 การตรวจสอบย้อนกลับของเวลา

4. กรณีการใช้งานของการประทับเวลาอิเล็กทรอนิกส์

การประทับเวลาอิเล็กทรอนิกส์หรือโทเคนประทับเวลา ไม่ได้แสดงค่าเวลาที่แน่นอนในขณะที่มีการสร้าง แก้ไข หรือลงลายมือชื่อต่อเอกสารอิเล็กทรอนิกส์ บุคคลที่สร้างเอกสารที่ต้องการนำไปประทับเวลาอาจลงลายมือชื่อต่อเอกสารดังกล่าวก่อนหรือหลังการประทับเวลาโดย TSA ก็ได้ โดย TSA จะเชื่อมโยงค่าเวลากับค่าแฮชของเอกสาร (อาจเป็นเอกสารที่ลงลายมือชื่อหรือเอกสารที่ยังไม่ลงลายมือชื่อ) เพื่อให้มีหลักฐานเพียงว่าเอกสารนั้นมีอยู่จริงหรือเกิดขึ้นก่อนการประทับเวลาเท่านั้น

อย่างไรก็ตาม การประทับเวลาอิเล็กทรอนิกส์มีคุณสมบัติที่ช่วยรับรองความถูกต้องของเวลาและวันที่ตามที่ระบุในโทเคนประทับเวลา และช่วยรักษาความครบถ้วนของข้อมูล (data integrity) ที่เชื่อมโยงกับเวลาและวันที่ดังกล่าว ทั้งนี้ บุคคลที่ได้รับข้อมูลที่ประทับเวลาแล้วสามารถตรวจสอบค่าเวลาที่ถูกต้องจากโทเคนประทับเวลา และยังสามารถตรวจสอบความน่าเชื่อถือของข้อมูลที่ประทับเวลาแล้วในระยะยาวได้ ดังนั้น การประทับเวลาอิเล็กทรอนิกส์จึงสามารถนำไปใช้ประโยชน์ได้หลายด้าน โดยตัวอย่างกรณีการใช้งานของการประทับเวลาอิเล็กทรอนิกส์ มีดังต่อไปนี้

4.1 การใช้งานการประทับเวลาอิเล็กทรอนิกส์ร่วมกับลายมือชื่ออิเล็กทรอนิกส์

การประทับเวลาอิเล็กทรอนิกส์สามารถนำไปใช้ร่วมกับลายมือชื่ออิเล็กทรอนิกส์ได้ 3 กรณีที่แตกต่างกันขึ้นอยู่กับเวลาในขณะที่มีการประทับเวลาและการลงลายมือชื่อเกิดขึ้น กล่าวคือ ข้อมูลอาจจะมีการประทับเวลา (1) ก่อนการลงลายมือชื่อโดยผู้ขอประทับเวลา (2) หลังการลงลายมือชื่อโดยผู้ขอประทับเวลา และ (3) ก่อนและหลังการลงลายมือชื่อโดยผู้ขอประทับเวลา โดยการประทับเวลาในแต่ละกรณีจะทำให้เกิดผลลัพธ์เป็นค่าเวลาของการลงลายมือชื่อที่แตกต่างกันตามตารางที่ 1

ตารางที่ 1 ลำดับเวลาของการประทับเวลาและการลงลายมือชื่อ

กรณี	ลำดับเหตุการณ์	ผลลัพธ์
กรณีที่ 1	(1) TSA สร้างโทเคนประทับเวลา (2) ผู้ขอประทับเวลา ลงลายมือชื่อต่อข้อมูลและโทเคนประทับเวลา	การประทับเวลาไม่ได้แสดงค่าเวลาในขณะที่มีการลงลายมือชื่อต่อข้อมูล แต่ยืนยันว่าลายมือชื่อเกิดขึ้นหลังเวลาที่ระบุในโทเคนประทับเวลา
กรณีที่ 2	(1) ผู้ขอประทับเวลา ลงลายมือชื่อต่อข้อมูล (2) TSA ประทับเวลาต่อข้อมูลที่ลงลายมือชื่อแล้ว	การประทับเวลายืนยันว่าลายมือชื่อเกิดขึ้นก่อนเวลาที่ระบุในโทเคนประทับเวลา
กรณีที่ 3	(1) TSA สร้างโทเคนประทับเวลา (2) ผู้ขอประทับเวลา ลงลายมือชื่อต่อข้อมูลและโทเคนประทับเวลา (3) TSA ประทับเวลาต่อข้อมูลที่ลงลายมือชื่อแล้ว	การประทับเวลายืนยันว่าลายมือชื่อเกิดขึ้นภายในช่วงเวลาระหว่างเวลาที่ระบุในโทเคนประทับเวลาสองอัน

ทั้งนี้ ข้อมูลที่ลงลายมือชื่อจะต้องมีการเก็บรักษาข้อมูลให้มีความครบถ้วน โดยการรักษาความครบถ้วนของข้อมูลสามารถใช้บุคคลที่สามที่เชื่อถือได้เป็นเสมือนพยานในการรับรองความครบถ้วนของข้อมูลด้วยการใช้ลายมือชื่อดิจิทัลของบุคคลดังกล่าว [1] กล่าวคือ ในการใช้งานการประทับเวลาอิเล็กทรอนิกส์ร่วมกับลายมือชื่ออิเล็กทรอนิกส์ทั่วไป การรักษาความครบถ้วนของข้อมูลสามารถอาศัยคุณสมบัติด้านความมั่นคงปลอดภัยของการประทับเวลาอิเล็กทรอนิกส์ ซึ่งใช้ TSA เป็นเสมือนพยานในการรับรองความครบถ้วนของข้อมูลที่ประทับเวลาแล้วด้วยการใช้ลายมือชื่อดิจิทัลของ TSA

4.2 การระบุเวลาที่น่าเชื่อถือของการออกเอกสารหรือการลงลายมือชื่อ

ในกระบวนการออกเอกสารอิเล็กทรอนิกส์หรือการลงลายมือชื่อต่อเอกสารอิเล็กทรอนิกส์ แม้ว่าเจ้าของลายมือชื่อจะใช้ลายมือชื่อดิจิทัลซึ่งมีคุณสมบัติที่ช่วยให้สามารถยืนยันตัวเจ้าของลายมือชื่อ (authentication) และตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้ (data integrity) รวมถึงทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเองลงลายมือชื่อได้ (non-repudiation) ก็ตาม บุคคลที่ได้รับเอกสารดังกล่าวจะไม่สามารถทราบอย่างชัดเจนถึงเวลาที่แน่นอนของการออกเอกสารหรือการลงลายมือชื่อ นอกจากนี้ เจ้าของลายมือชื่ออาจเลือกระบุเวลาของการออกเอกสารหรือการลงลายมือชื่อเป็นเวลาใดก็ได้ (เช่น เวลาของเครื่องคอมพิวเตอร์ที่กำลังใช้งาน) หากไม่มีการประทับเวลาที่น่าเชื่อถือ ดังนั้น การประทับเวลาอิเล็กทรอนิกส์เพื่อใช้ระบุเวลาที่น่าเชื่อถือของการออกเอกสารหรือการลงลายมือชื่อจะช่วยป้องกันปัญหาข้อพิพาทเกี่ยวกับความถูกต้องของเวลาและวันที่

ตัวอย่างของเอกสารอิเล็กทรอนิกส์ที่อาจจำเป็นต้องใช้การระบุเวลาที่น่าเชื่อถือของการออกเอกสารหรือการลงลายมือชื่อ เช่น

- เอกสารทางการของหน่วยงานภาครัฐ เช่น ระเบียบ ข้อบังคับ ประกาศ คำสั่ง และหนังสือภายนอก
- เอกสารเกี่ยวกับกระบวนการจัดซื้อจัดจ้างภาครัฐหรือการยื่นประมูลงาน ซึ่งกำหนดกรอบเวลาที่เข้มงวด
- เอกสารเกี่ยวกับกระบวนการพิจารณาคดี ซึ่งกำหนดกรอบเวลาที่เข้มงวด
- สัญญาที่ต้องระบุเวลาที่แน่นอนของการลงลายมือชื่อ เช่น สัญญาประกันความเสียหาย สัญญาเช่า และสัญญาซื้อขาย
- เอกสารที่ต้องยื่นต่อหน่วยงานภาครัฐ ซึ่งจำเป็นต้องลงลายมือชื่อโดยผู้มีอำนาจทำการในขณะนั้น
- เอกสารที่ออกต่อเนื่องตามลำดับเวลา เช่น ใบกำกับภาษี ซึ่งระบุวันที่และเลขที่ตามลำดับเวลา

4.3 การเก็บรักษาข้อมูลและลายมือชื่อในระยะยาว

ข้อมูลหรือเอกสารอิเล็กทรอนิกส์บางประเภทจำเป็นต้องมีการเก็บรักษาข้อมูลเป็นระยะเวลานาน โดยคู่กรณีที่เกี่ยวข้องยังสามารถตรวจสอบความถูกต้องของลายมือชื่ออิเล็กทรอนิกส์บนข้อมูลนั้นได้ เนื่องจากต้องการอาศัยผลทางกฎหมายของลายมือชื่ออิเล็กทรอนิกส์เป็นระยะเวลานาน

การประทับเวลาอิเล็กทรอนิกส์สามารถช่วยให้สามารถเก็บรักษาข้อมูลและลายมือชื่อในระยะยาวได้ โดยเริ่มจากการสร้างโทเคนประทับเวลาเพื่อรักษาความครบถ้วนของข้อมูลและลายมือชื่อ จากนั้น สามารถต่ออายุหรือขยายช่วงเวลาใช้งานได้ของโทเคนประทับเวลาอันเดิม (ด้วยการตรวจสอบความถูกต้องของโทเคนประทับเวลาอันเดิมและการสร้างโทเคนประทับเวลาอันใหม่) ออกไปเป็นระยะตลอดช่วงเวลาของการเก็บรักษาข้อมูล เพื่อให้บุคคลที่เก็บรักษาข้อมูลในระยะยาวสามารถยืนยันได้ว่าข้อมูลดังกล่าวเป็นข้อมูลที่ลงลายมือชื่อซึ่งเป็นต้นฉบับ

5. แนวนโยบายการประทับเวลา

แนวนโยบายการประทับเวลา (time-stamp policy) เป็นชุดของข้อกำหนดที่บ่งบอกถึงการบังคับใช้งานโทเคนประทับเวลาในกลุ่มการใช้งานที่มีข้อกำหนดด้านความมั่นคงปลอดภัยร่วมกัน

ข้อเสนอแนะมาตรฐานฉบับนี้ กำหนดข้อกำหนดสำหรับแนวนโยบายการประทับเวลาพื้นฐาน สำหรับ TSA ที่ออกโทเคนประทับเวลาโดยอาศัยใบรับรองกุญแจสาธารณะ ใช้วิธีการประสานเวลากับมาตรเวลาร่วมสากลในการออกโทเคนประทับเวลาด้วยค่าความแม่นยำของเวลาที่ 1 วินาทีหรือดีกว่า และมีการลงลายมือชื่อดิจิทัลลงบนโทเคนประทับเวลา ทั้งนี้ TSA อาจกำหนดแนวนโยบายของตนเองก็ได้ โดยแนวนโยบายนั้นต้องครอบคลุมข้อกำหนดของแนวนโยบายตามข้อเสนอแนะมาตรฐานฉบับนี้ หรือมีข้อกำหนดเพิ่มเติมได้

ในกรณีที่ TSA ให้บริการประทับเวลาโดยค่าเวลาที่ใช้ในการประทับมีค่าความแม่นยำที่ดีกว่า 1 วินาที TSA จะต้องระบุค่าความแม่นยำดังกล่าวไว้ในคำชี้แจงการเปิดเผยข้อมูล และทุกโทเคนประทับเวลาต้องมีค่าเวลาที่มีค่าความแม่นยำเท่ากันตามที่ระบุไว้

5.1 การระบุแนวนโยบาย (identification)

TSA ต้องเปิดเผยค่าระบุแนวนโยบายการประทับเวลาที่นำมาใช้ในคำชี้แจงการเปิดเผยข้อมูลของผู้ให้บริการประทับเวลาต่อผู้ใช้บริการและคู่กรณีที่เกี่ยวข้อง (relying party) ซึ่งเป็นบุคคลที่เชื่อถือโทเคนประทับเวลา เพื่อแสดงให้เห็นถึงความสอดคล้องของการให้บริการ

5.2 กลุ่มผู้ใช้งานและการใช้งาน (user community and applicability)

แนวนโยบายการประทับเวลานี้มุ่งหวังให้การให้บริการเป็นไปตามข้อกำหนดของการประทับเวลาในลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้เพื่อความถูกต้องในระยะยาว แต่สามารถนำไปประยุกต์ใช้กับการใช้ประโยชน์ในด้านอื่นได้เช่นกัน

แนวนโยบายนี้อาจนำไปใช้สำหรับการให้บริการประทับเวลาแบบสาธารณะ (public time-stamping service) หรือการให้บริการประทับเวลาภายในกลุ่มผู้ใช้งานเฉพาะ (closed community) ก็ได้

5.3 ความสอดคล้อง (conformance)

TSA ต้องใช้ค่าระบุแนวนโยบายการประทับเวลา (ตามที่กำหนดใน ข้อ 5.1) เป็นข้อมูลหนึ่งในโทเคนประทับเวลา หาก TSA อ้างถึงความสอดคล้องต่อแนวนโยบายการประทับเวลาที่ระบุไว้ TSA ต้องสามารถแสดงหลักฐานเพื่อสนับสนุนข้อกล่าวอ้างถึงความสอดคล้องนั้นต่อผู้ใช้บริการและคู่กรณีที่เกี่ยวข้องเมื่อมีการร้องขอได้

6. แนวปฏิบัติของผู้ให้บริการประทับเวลา

เพื่อให้การให้บริการของ TSA มีความน่าเชื่อถือ และสอดคล้องตามมาตรฐานสากล นอกจากการกำหนดแนวนโยบายการประทับเวลา TSA ต้องจัดทำแนวปฏิบัติของผู้ให้บริการประทับเวลา (TSA practice statement) สำหรับการให้บริการประทับเวลา และต้องทำให้มั่นใจว่าได้นำข้อกำหนดแนวปฏิบัติทั้งหมดมาปฏิบัติตามแนวนโยบายการประทับเวลาที่ได้เลือกใช้ โดยแนวปฏิบัติของผู้ให้บริการประทับเวลานั้น ต้องได้รับการอนุมัติจากคณะผู้บริหารระดับสูงก่อนนำไปใช้งานและเผยแพร่ให้ผู้ที่เกี่ยวข้องได้รับทราบ เพื่อให้ผู้ใช้บริการและคู่กรณีที่เกี่ยวข้อง สามารถประเมินได้ด้วยตนเองว่า TSA มีความน่าเชื่อถือเพียงพอต่อความต้องการในการใช้งานหรือไม่

TSA ต้องทำการควบคุมการให้บริการประทับเวลา ให้เป็นไปตามข้อกำหนดในเอกสารฉบับนี้ ซึ่งเป็นข้อกำหนดภายใต้วัตถุประสงค์ด้านความมั่นคงปลอดภัยที่ TSA ต้องนำมาปฏิบัติเพื่อดำเนินการให้บรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยที่กำหนดไว้ โดยรายละเอียดของการควบคุมตามข้อกำหนดเพื่อให้เป็นไปตามวัตถุประสงค์นั้น คือความสมดุลระหว่างการให้บริการด้วยระดับความมั่นคงปลอดภัยที่เพียงพอ ในขณะที่ลดข้อจำกัดในด้านเทคนิคที่ผู้ให้บริการอาจนำมาใช้ในการประทับเวลา

ข้อกำหนดในส่วนที่เกี่ยวข้องกับการตอบสนอง (response) ต่อคำขอใช้บริการประทับเวลานั้น ขึ้นอยู่กับดุลยพินิจของ TSA ตามข้อตกลงระดับการให้บริการ (service level agreements) ที่ทำไว้ร่วมกับผู้ใช้บริการ

6.1 คำชี้แจงเกี่ยวกับแนวปฏิบัติและการเปิดเผยข้อมูล

6.1.1 คำชี้แจงแนวปฏิบัติของผู้ให้บริการประทับเวลา

TSA ต้องแสดงให้เห็นถึงแนวปฏิบัติที่ชัดเจน เพื่อทำให้มั่นใจว่าการให้บริการประทับเวลานั้นมีความน่าเชื่อถือ โดยเฉพาะอย่างยิ่ง ในหัวข้อดังต่อไปนี้

(1) TSA ต้องประเมินความเสี่ยงเกี่ยวกับความมั่นคงปลอดภัยของสินทรัพย์ที่สำคัญในการให้บริการและภัยคุกคามต่อสินทรัพย์เหล่านั้น เพื่อประเมินและกำหนดแผนการควบคุมความมั่นคงปลอดภัยและขั้นตอนการปฏิบัติงานที่จำเป็นสำหรับการจัดการความเสี่ยงนั้น

(2) TSA ต้องมีคำชี้แจงการปฏิบัติและขั้นตอนที่ใช้ในการดำเนินงานตามข้อกำหนดทั้งหมดที่ระบุไว้ในแนวนโยบายการประทับเวลานี้

หมายเหตุ: แนวนโยบายการประทับเวลานี้ไม่ได้ระบุข้อกำหนดของโครงสร้างหรือหัวข้อที่ต้องกำหนดไว้ในแนวปฏิบัติของ TSA

(3) คำชี้แจงแนวปฏิบัติของ TSA จะต้องระบุภาระผูกพันขององค์กรภายนอกทั้งหมดที่สนับสนุนการให้บริการของ TSA รวมถึงแนวนโยบายและแนวปฏิบัติที่เกี่ยวข้อง

(4) TSA ต้องเผยแพร่คำชี้แจงแนวปฏิบัติและเอกสารอื่นใดที่เกี่ยวข้อง ให้ผู้ใช้บริการและคู่กรณีที่เกี่ยวข้อง รับทราบตามความจำเป็น เพื่อให้สามารถประเมินได้ว่าแนวปฏิบัติของผู้ให้บริการนั้นมีความสอดคล้องกับนโยบายการประทับเวลาที่กำหนดไว้หรือไม่

หมายเหตุ: TSA ไม่จำเป็นต้องเผยแพร่รายละเอียดแนวปฏิบัติทั้งหมด

(5) TSA ต้องเปิดเผยข้อกำหนดและเงื่อนไขที่เกี่ยวข้องกับการใช้บริการการประทับเวลา ให้ผู้ใช้บริการและคู่กรณีที่เกี่ยวข้องรับทราบ ตามที่ระบุไว้ในคำชี้แจงการเปิดเผยข้อมูล

(6) คำชี้แจงแนวปฏิบัติของ TSA ต้องผ่านการอนุมัติจากคณะผู้บริหารระดับสูงซึ่งเป็นผู้มีอำนาจสูงสุดของหน่วยงาน

(7) ผู้บริหารระดับสูงของ TSA ต้องทำให้มั่นใจว่ามีการนำแนวปฏิบัติไปดำเนินการอย่างเหมาะสม

(8) TSA ต้องกำหนดกระบวนการสำหรับทบทวนแนวปฏิบัติรวมถึงความรับผิดชอบในการดำเนินการตามคำชี้แจงแนวปฏิบัติที่ได้กำหนดไว้

(9) ในกรณีที่จะมีการเปลี่ยนแปลงข้อมูลในคำชี้แจงแนวปฏิบัติ TSA ต้องแจ้งให้ผู้ที่มีส่วนเกี่ยวข้องรับทราบล่วงหน้าถึงการเปลี่ยนแปลงในคำชี้แจงแนวปฏิบัติ และหลังจากได้รับการอนุมัติตามข้อ (6) แล้ว จะต้องจัดทำคำชี้แจงแนวปฏิบัติฉบับแก้ไขในทันทีตามที่กำหนดข้างต้นใน ข้อ (4)

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.1.1. TSA Practice Statement

6.1.2 คำชี้แจงการเปิดเผยข้อมูลของผู้ให้บริการประทับเวลา

TSA ต้องเปิดเผยข้อกำหนดและเงื่อนไขเกี่ยวกับการใช้บริการประทับเวลาของ TSA ต่อผู้ใช้บริการและคู่กรณีที่เกี่ยวข้อง โดยคำชี้แจงนี้ต้องระบุแนวนโยบายการประทับเวลาที่ TSA นำมาใช้เป็นอย่างน้อย

(1) ข้อมูลการติดต่อ TSA

(2) แนวนโยบายการประทับเวลาที่นำมาใช้

(3) อัลกอริทึมสำหรับสร้างค่าแฮชอย่างน้อยหนึ่งอัลกอริทึม ซึ่งอาจมีการใช้แทนข้อมูลที่ถูกประทับเวลา

(4) อายุการใช้งานที่คาดหมายไว้ของลายมือชื่อที่ใช้ในการลงลายมือชื่อโทเคนประทับเวลา (ทั้งนี้ จะยาวนานเท่าใดขึ้นอยู่กับอัลกอริทึมที่ใช้ในการแฮชหรือลงลายมือชื่อ และความยาวของกุญแจส่วนตัว)

(5) ความแม่นยำของค่าเวลาในโทเคนประทับเวลาเมื่อเทียบกับมาตรเวลาร่วมสากล

(6) ข้อจำกัดในการใช้บริการประทับเวลา

(7) ภาระผูกพันของผู้ใช้บริการ (ถ้ามี)

(8) ภาระผูกพันของคู่กรณีที่เกี่ยวข้อง

(9) ข้อมูลเกี่ยวกับวิธีการตรวจสอบโทเคนประทับเวลา และข้อจำกัดที่อาจเกิดขึ้นได้ในช่วงเวลาที่มีผลบังคับใช้ (validity period)

(10) ระยะเวลาที่บันทึกเหตุการณ์ (event logs) จะถูกเก็บรักษาไว้

(11) ข้อกำหนดและกฎหมายที่เกี่ยวข้องกับการให้บริการประทับเวลาในประเทศไทย

(12) ข้อจำกัดความรับผิด

(13) ขั้นตอนการร้องเรียนและกระบวนการระงับข้อพิพาท

(14) หาก TSA ได้รับการประเมินว่ามีความสอดคล้องกับแนวนโยบายการประทับเวลาที่ระบุไว้ จะต้องระบุหน่วยงานที่ทำการประเมินด้วย

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.1.2. TSA Disclosure Statement

6.2 วงจรการบริหารจัดการกุญแจ

6.2.1 การสร้างกุญแจเข้ารหัส

TSA ต้องทำให้มั่นใจว่ากุญแจเข้ารหัส (cryptographic key) ถูกสร้างขึ้นภายใต้สถานการณ์ที่มีการควบคุม ต้องดำเนินการภายใต้สภาพแวดล้อมที่มีความมั่นคงปลอดภัยทางกายภาพ โดยบุคลากรที่ได้รับมอบหมายเท่านั้น อย่างน้อยที่สุดต้องมีการควบคุมแบบ dual control

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.2.1. TSA Key Generation

6.2.2 การป้องกันกุญแจส่วนตัว

TSA ต้องทำให้มั่นใจว่ากุญแจส่วนตัวถูกจัดเก็บไว้เป็นความลับ (confidential) และคงความครบถ้วนสมบูรณ์ (integrity)

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.2.2. TSU Private Key Protection

6.2.3 การเผยแพร่กุญแจสาธารณะ

TSA ต้องทำให้มั่นใจว่าความสมบูรณ์และความถูกต้อง (integrity and authenticity) ของกุญแจสาธารณะสำหรับการตรวจสอบลายมือชื่อ และพารามิเตอร์ที่เกี่ยวข้องจะคงอยู่ ในระหว่างการเผยแพร่ให้กับคู่กรณีที่เกี่ยวข้อง

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.2.3. TSU Public Key Distribution

6.2.4 การรับรองกุญแจคู่ใหม่

TSA ต้องทำให้มั่นใจว่าอายุการใช้งานของใบรับรอง ต้องไม่เกินกว่าระยะเวลาที่อัลกอริทึมและความยาวของกุญแจที่เลือกใช้ได้รับการยอมรับว่าเหมาะสมกับวัตถุประสงค์ในการใช้งาน หากเกิดกรณีของการเพิกถอนใบรับรอง TSA ต้องใช้กุญแจคู่ใหม่

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.2.4. Rekeying TSU's Key

6.2.5 การหมดอายุการใช้งานของคู่กุญแจ

TSA ต้องทำให้มั่นใจว่ากุญแจส่วนตัวสำหรับการลงลายมือชื่อ จะไม่ถูกนำมาใช้ภายหลังกุญแจหมดอายุการใช้งาน

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.2.5. End of TSU Key Life Cycle

6.2.6 การบริหารจัดการวงจรการใช้งานของอุปกรณ์เข้ารหัสลับที่ใช้ลงลายมือชื่อต่อโทเคนประทับเวลา

TSA ต้องทำให้มั่นใจในความมั่นคงปลอดภัยของอุปกรณ์เข้ารหัสลับ ตลอดวงจรการใช้งานของอุปกรณ์นั้น

- อุปกรณ์เข้ารหัสสำหรับการลงลายมือชื่อโทเคนประทับเวลา ต้องไม่ถูกดัดแปลงระหว่างการขนส่งและการเก็บรักษา
- การติดตั้ง การเปิดใช้งาน และการทำสำเนาของกุญแจส่วนตัวในการลงลายมือชื่อโดยอุปกรณ์เข้ารหัส ต้องดำเนินการโดยบุคลากรที่ได้รับมอบหมายเท่านั้น โดยอย่างน้อยที่สุดต้องมีการควบคุมแบบ dual control ภายในสภาพแวดล้อมที่มีการรักษาความปลอดภัยทางภาพภาพ
- กุญแจส่วนตัวในการลงลายมือชื่อที่จัดเก็บไว้ในอุปกรณ์เข้ารหัสต้องถูกทำลายเมื่อยกเลิกการใช้งานอุปกรณ์

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.2.6. Life Cycle Management of the Cryptographic Module used to Sign Time-Stamps

6.3 การประทับเวลา

6.3.1 โทเคนประทับเวลา

TSA ต้องทำให้มั่นใจว่าโทเคนประทับเวลานั้นได้รับการออกอย่างมั่นคงปลอดภัย และประกอบด้วยค่าเวลาที่ถูกต้อง

(1) โทเคนประทับเวลาต้องประกอบด้วยค่าระบุแนวนโยบายการประทับเวลา
(2) โทเคนประทับเวลาแต่ละโทเคน ต้องมีค่าระบุเฉพาะโทเคน
(3) ค่าเวลาในโทเคนประทับเวลา ต้องสามารถตรวจสอบกลับได้กับอย่างน้อยหนึ่งค่าเวลาจริงที่เผยแพร่โดย UTC(k)
(4) ค่าเวลาในโทเคนประทับเวลา ต้องสอดคล้องกับมาตรเวลาร่วมสากลตามค่าความแม่นยำที่กำหนดไว้ในแนวนโยบายนี้ และค่าความแม่นยำของค่าเวลาที่ระบุไว้ในโทเคนประทับเวลา (ถ้ามี)

(5) หากตรวจพบว่าค่าเวลาของนาฬิกาที่ให้บริการประทับเวลานั้นขาดความแม่นยำตามที่กำหนดไว้ ต้องไม่ทำการออกโทเคนประทับเวลา

(6) โทเคนประทับเวลา ต้องมีค่าแฮชของข้อมูลที่จะประทับเวลา ที่ผู้ขอประทับเวลาส่งมาเพื่อขอประทับเวลาประกอบอยู่ด้วย

(7) โทเคนประทับเวลาต้องถูกลงลายมือชื่อโดยใช้กุญแจที่สร้างมาเพื่อวัตถุประสงค์นี้โดยเฉพาะ

(8) โทเคนประทับเวลาต้องประกอบด้วย

- ค่าระบุประเทศที่ตั้งของ TSA
- ค่าระบุตัวตนของ TSA ที่ให้บริการ
- ค่าระบุตัวตนของหน่วยที่ทำการออกโทเคนประทับเวลา

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.3.1. Time-Stamp Token

6.3.2 ความสอดคล้องของเวลากับมาตรเวลาร่วมสากล

TSA ต้องทำให้มั่นใจว่านาฬิกาของตนเองมีการเทียบเวลาและสอดคล้องกับมาตรเวลาร่วมสากลตามค่าความแม่นยำที่กำหนด

(1) การเทียบเวลาของนาฬิกาที่ใช้ออกโทเคนประทับเวลานั้นต้องได้รับการดูแลรักษาให้คงค่าความแม่นยำตามที่กำหนดไว้

(2) นาฬิกาที่ใช้ออกโทเคนประทับเวลาต้องได้รับการป้องกันจากภัยคุกคามที่อาจส่งผลให้นาฬิกานั้นเกิดความเปลี่ยนแปลงที่ไม่สามารถตรวจพบได้ ซึ่งทำให้ค่าเวลาไม่ถูกต้องตามที่ได้มีการเทียบเวลาไว้

(3) TSA ต้องทำให้มั่นใจว่า สามารถตรวจพบได้หากข้อมูลค่าเวลาในโทเคนประทับเวลานั้น ไม่สอดคล้องกับมาตรเวลาร่วมสากล

(4) TSA ต้องทำให้มั่นใจว่า มีการปรับเทียบเวลาเมื่อเกิดวินาทีทด (leap second)[3] ตามที่มีแจ้งการเปลี่ยนแปลงเวลามาตรฐานโดยหน่วยงานผู้รับผิดชอบในการรักษามาตรฐานทางด้านเวลาเพื่อให้สอดคล้องกับการปรับเวลาตามมาตรฐานสากล การปรับวินาทีทดจะเกิดขึ้นในช่วงนาทีสุดท้ายของวันที่จะทำการเปลี่ยนแปลงเวลา TSA ต้องทำการบันทึกเหตุการณ์การเปลี่ยนแปลงเวลาที่เกิดขึ้นด้วย

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.3. 2. Clock Synchronization with UTC

[3] วินาทีทด (leap second) เป็นการเพิ่มหรือลดวินาทีเข้าไปในมาตรเวลาร่วมสากล ซึ่งเป็นวิธีการที่ทำให้เวลามาตรฐานโลกสอดคล้องกับการหมุนของโลก

6.4 การบริหารจัดการและการดำเนินการของผู้ให้บริการประทับเวลา

6.4.1 การบริหารจัดการความมั่นคงปลอดภัย

TSA ต้องทำให้มั่นใจว่าขั้นตอนและกระบวนการบริหารจัดการความมั่นคงปลอดภัยของการให้บริการนั้น เพียงพอและสอดคล้องกับแนวปฏิบัติที่เป็นเลิศที่ได้รับการยอมรับ

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.4.1. Security Management

6.4.2 การจำแนกและการบริหารจัดการสินทรัพย์

TSA ต้องทำให้มั่นใจว่าการป้องกันข้อมูลและสินทรัพย์อื่น ๆ มีระดับการป้องกันที่มีความเหมาะสม

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.4.2. Asset Classification and Management

6.4.3 การรักษาความมั่นคงปลอดภัยทางบุคลากร

TSA ต้องทำให้มั่นใจว่าบุคลากรและแนวปฏิบัติในการว่าจ้างนั้น ส่งเสริมและสนับสนุนความน่าเชื่อถือในการดำเนินงานของ TSA

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.4.3. Personnel Security

6.4.4 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

TSA ต้องทำให้มั่นใจว่ามีการควบคุมการเข้าถึงบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย และลดความเสี่ยงทางกายภาพที่อาจเกิดต่อสินทรัพย์ของ TSA

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.4.4. Physical and Environmental Security

6.4.5 การบริหารจัดการการดำเนินงาน

TSA ต้องทำให้มั่นใจว่าองค์ประกอบของระบบมีความมั่นคงปลอดภัย และดำเนินการได้อย่างถูกต้อง โดยมีความเสี่ยงที่จะล้มเหลวในระดับต่ำสุด

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.4.5. Operations Management

6.4.6 การบริหารจัดการการเข้าถึงระบบ

TSA ต้องทำให้มั่นใจว่าการเข้าถึงระบบของ TSA จำกัดเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.4.6. System Access Management

6.4.7 การติดตั้งและดูแลรักษาระบบที่น่าเชื่อถือ

TSA ต้องใช้ระบบและผลิตภัณฑ์ที่น่าเชื่อถือ ซึ่งมีการป้องกันการดัดแปลงแก้ไข

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.4.7. Trustworthy Systems Deployment and Maintenance

6.4.8 พฤติการณ์ที่กระทบต่อความมั่นคงปลอดภัยของการให้บริการของ TSA

TSA ต้องทำให้มั่นใจว่า ในกรณีที่เกิดเหตุการณ์ที่ส่งผลกระทบด้านความมั่นคงปลอดภัยต่อการให้บริการของ TSA รวมไปถึงพฤติการณ์ที่กระทบต่อความมั่นคงปลอดภัยของข้อมูลกุญแจลงนามส่วนตัว หรือตรวจพบการสูญเสียของการเทียบเวลา ข้อมูลที่เกี่ยวข้องดังกล่าวจะต้องถูกเปิดเผยต่อผู้ใช้บริการและหน่วยงานที่พึ่งพาอาศัย

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.4.8. Compromise of TSA Services

6.4.9 การยุติการให้บริการของ TSA

TSA ต้องลดความเสี่ยงการหยุดชะงักของบริการที่อาจเกิดขึ้นกับผู้ใช้บริการหรือคู่กรณีที่เกี่ยวข้องจากการยุติการให้บริการประทับเวลาของ TSA โดยเฉพาะอย่างยิ่ง TSA ต้องดูแลรักษาข้อมูลที่สำคัญในการตรวจสอบความถูกต้องของโทเคนประทับเวลา

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.4.9. TSA Termination

6.4.10 การปฏิบัติตามข้อกำหนดทางกฎหมาย

TSA ต้องปฏิบัติตามข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.4.10. Compliance with Legal Requirements

6.4.11 การบันทึกข้อมูลที่เกี่ยวข้องกับการดำเนินการให้บริการประทับเวลา

TSA ต้องทำให้มั่นใจว่า ข้อมูลที่เกี่ยวข้องทั้งหมดเกี่ยวกับการให้บริการประทับเวลา ถูกบันทึกและเก็บไว้ตามระยะเวลาที่กำหนด โดยเฉพาะอย่างยิ่งเพื่อวัตถุประสงค์ในการใช้เป็นหลักฐานทางกฎหมาย

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.4.11. Recording of Information Concerning Operation of Time-Stamping Services

6.5 การบริหารจัดการองค์กร

TSA ต้องทำให้มั่นใจว่าเป็นหน่วยงานที่มีความน่าเชื่อถือ โดยต้องจดทะเบียนเป็นนิติบุคคลตามกฎหมาย มีเอกสารข้อตกลงและความสัมพันธ์ทางสัญญา หากการให้บริการมีการรับเหมาช่วง การจ้างภายนอก หรือข้อตกลงอื่นของบุคคลที่สามมาเกี่ยวข้อง TSA ต้องจัดให้มีจำนวนบุคลากรที่เพียงพอ โดยบุคลากรได้รับการศึกษา การฝึกอบรม มีความรู้ด้านเทคนิคและประสบการณ์ที่จำเป็นเกี่ยวกับประเภท ขอบเขต และปริมาณของงานที่จำเป็นสำหรับการให้บริการประทับเวลา

แนวนโยบายและขั้นตอนการปฏิบัติงานของ TSA จะต้องไม่ก่อให้เกิดการเลือกปฏิบัติ โดย TSA จะต้องให้บริการที่เข้าถึงได้สำหรับผู้ขอใช้บริการทุกราย ที่ตกลงและยอมรับภาระผูกพันของผู้ใช้บริการ ตามที่ระบุไว้ในคำชี้แจงการเปิดเผยข้อมูลของ TSA รวมไปถึงการกำหนดแนวนโยบายและขั้นตอนในการแก้ไขข้อร้องเรียนและข้อพิพาทที่ได้รับจากผู้ใช้บริการ เกี่ยวกับการให้บริการประทับเวลาหรือเรื่องอื่น ๆ ที่เกี่ยวข้อง

รายละเอียดให้เป็นไปตาม RFC 3628 ข้อ 7.5. Organizational

440 **บรรณานุกรม**

441

[1] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยแนวทางการลงลายมือชื่ออิเล็กทรอนิกส์ เลขที่ ขมธอ. 23-2563, เวอร์ชัน 1.0.

[2] ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) พ.ศ. 2552.

[3] IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), August 2001.

[4] International Organization for Standardization, "ISO/IEC 18014-4:2015 Information technology – Security techniques – Time-stamping services – Part 4: Traceability of time sources", April 2015.

[5] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles", March 2016.

[6] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps", March 2016.

[7] IETF RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs), November 2003.

[8] International Organization for Standardization, "ISO/IEC 18014-1:2008 Information technology – Security techniques – Time-stamping services – Part 1: Framework", September 2008.

[9] International Organization for Standardization, "ISO/IEC 18014-2:2021 Information security – Time-stamping services – Part 2: Mechanisms producing independent tokens", September 2021.

[10] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม.

442