ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์
ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน

โดยที่เป็นการสมควรปรับปรุงข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้แนวทางการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความสอดคล้องกับบริบทการใช้งาน ความต้องการทางธุรกิจ และคุณลักษณะของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลในปัจจุบันของประเทศไทย

อาศัยอำนาจตามความในมาตรา ๕ แห่งพระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๒ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ จึงให้ยกเลิกประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน เลขที่ ขมธอ. ๑๘-๒๕๖๔ ลงวันที่ ๓๐ กันยายน ๒๕๖๔ และประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน เลขที่ ขมธอ. ๑๘-๒๕๖๖ ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๒๓ กุมภาพันธ์ พ.ศ. ๒๕๖๖

(นายศักดิ์ เสกขุนทด)
ที่ปรึกษา รักษาการในตำแหน่งรองผู้อำนวยการ
ปฏิบัติการแทนผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard

for Electronic Transactions

ขมธอ. 18-2566

ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน

DIGITAL IDENTITY – FRAMEWORK

เวอร์ชัน 3.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.030

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน

ขมธอ. 18-2566

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 23 กุมภาพันธ์ พ.ศ. 2566

คณะอนุกรรมการกลั่นกรองการกำหนดหลักเกณฑ์ในการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ประธานอนุกรรมการ

นางสาวอัจฉรินทร์ พัฒนพันธ์ชัย

อนุกรรมการ

นายอนันต์ กนกศิลป์	สำนักงานปลัดกระทรวงสาธารณสุข
นางรุ่งนิภา อมาตยคง	
นายสัญชัย เตชนิมิตวัช	กรมการปกครอง
นายอภิวัฒน์ อินขัด	กรมการกงสุล
นางศิริพร ชำนาญชาติ	กรมพัฒนาธุรกิจการค้า
นางสาวรัญศิกานต์ งามบุษบงโสภา	
นางสาวสิริธิดา พนมวัน ณ อยุธยา	ธนาคารแห่งประเทศไทย
นางสาววิจิตรเลขา มารมย์	
นางสาวสายชล แซ่ลี้	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
นางสาวจิตสถา ศรีประเสริฐสุข	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และ
นางสาวอรวรี เจริญพร	กิจการโทรคมนาคมแห่งชาติ
นายสมเกียรติ วัฒนาประสบสุข	สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
นายณัฐวุฒิ ทิพย์กนก	
นายณรงค์เดช วัชระภาสร	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
นายกิตตินันท์ ศรีมงคล	
นายวิบูลย์ ภัทรพิบูล	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
นายอภิสิทธิ์ สุขสาคร	
นายพีรธร วิมลโลหการ	สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นางสาวอุรัชฎา เกตุพรหม	
นายจำรัส สว่างสมุทร	คณะกรรมการร่วมภาคเอกชน ๓ สถาบัน
นายวิเชียร เปรมชัยสวัสดิ์	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นายณัฐวุฒิ อมรวิวัฒน์	

เลขานุการ

นางสาวพลอย เจริญสม	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คณะอนุกรรมการมาตรฐานและการกำกับดูแล

ประธานอนุกรรมการ

นายยรรยง เต็งอำนวย

อนุกรรมการ

รองศาสตราจารย์ปริทรรศน์ พันธุบรรยงก์	
นายปริญญา หอมเอนก	
นางสาวภรณี หรูวรรธนะ	
นายรอม หิรัญพฤกษ์	
นางสาวสุธีรา ศรีไพบูลย์	
นายอนุชิต อนุชิตานุกูล	
นางสาวสุดจิตร ลาภเลิศสุข	กรมบัญชีกลาง
นางสาวภิญญู กำเนิดหล่ม	กรมสรรพากร
นางสาวรัญศิกานต์ งามบุษบงโสภา	กรมพัฒนาธุรกิจการค้า
นายก่อเกียรติ แก้วกิ่ง	กรมการปกครอง
นางศิริพร ช่างการ	สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม
นายสมเกียรติ วัฒนาประสบสุข	สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
นายกำพล ศรธนะรัตน์	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
นายเนติพงษ์ ตลับนาค	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
นายสินชัย ต่อวัฒนกิจกุล	สำนักงานหลักประกันสุขภาพแห่งชาติ
นางบุษกร ธีระปัญญาชัย	ธนาคารแห่งประเทศไทย
นายภิญโญ ตรีเพชราภรณ์	
นายเอธ แย้มประทุม	
นายสุพจน์ เธียรวุฒิ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายวิบูลย์ ภัทรพิบูล	
นายวีระ วีระกุล	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นางสาวธิดารัช ธนภรรคภวิน	

อนุกรรมการและเลขานุการ

นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ช่วยเลขานุการ

นายสิริณัฐ ตั้งธรรมจิต	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงานฉบับนี้ จัดทำขึ้นเพื่ออธิบายคำศัพท์ กระบวนการ การประเมินความเสี่ยง และการกำหนดระดับความน่าเชื่อถือที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อให้ผู้ที่เกี่ยวข้องกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความเข้าใจตรงกัน

โดยมีการนำเสนอและรับฟังความคิดเห็นเป็นการทั่วไป ตลอดจนพิจารณาข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วนยิ่งขึ้น รวมทั้งให้สามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงานฉบับนี้ จัดทำขึ้นโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

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

การพิสูจน์และยืนยันตัวตนของบุคคลเป็นขั้นตอนสำคัญในการทำธุรกรรมในระบบเศรษฐกิจ แต่ที่ผ่านมาผู้ที่ประสงค์ขอรับบริการจากผู้ประกอบการหรือหน่วยงานใด ๆ จะต้องทำการพิสูจน์และยืนยันตัวตนโดยการแสดงตนต่อผู้ให้บริการพร้อมกับต้องส่งเอกสารหลักฐาน ซึ่งเป็นภาระต่อผู้ใช้บริการและผู้ให้บริการ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชนจึงได้ร่วมกันจัดทำมาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัล เป็นข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ (ETDA Recommendation) เวอร์ชัน 1.0 (เลขที่ ขมธอ. 18-2561, 19-2561 และ 20-2561) และเวอร์ชัน 2.0 (เลขที่ ขมธอ. 18-2564, 19-2564 และ 20-2564)

ทั้งนี้ กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์กำหนดให้บุคคลสามารถพิสูจน์และยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ โดยมีกลไกการควบคุมดูแลผู้ประกอบธุรกิจบริการที่เกี่ยวข้องเพื่อให้ระบบดังกล่าวมีความน่าเชื่อถือและปลอดภัย ป้องกันความเสียหายที่อาจเกิดขึ้นต่อสาธารณชน ตลอดจนเสริมสร้างความน่าเชื่อถือและการยอมรับในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ในการนี้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์จึงได้แก้ไขปรับปรุงข้อเสนอแนะมาตรฐานฯ ฉบับเดิม เพื่อให้แนวทางการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความสอดคล้องกับบริบทการใช้งาน ความต้องการทางธุรกิจและคุณลักษณะของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลในประเทศไทย โดยจัดทำเป็นข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อมาใช้แทนข้อเสนอแนะมาตรฐานฯ ฉบับเดิม และยกเลิกข้อเสนอแนะมาตรฐานฯ ฉบับเดิม (ข้อเสนอแนะมาตรฐานฯ เลขที่ ขมธอ. 18-2564 ขมธอ. 19-2564 และ ขมธอ. 20-2564)

ข้อเสนอแนะมาตรฐานฉบับนี้เป็นส่วนหนึ่งของชุดข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งประกอบด้วย

(1) ข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน (เวอร์ชัน 3.0)
(2) ข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน (เวอร์ชัน 3.0)
(3) ข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการยืนยันตัวตน (เวอร์ชัน 3.0)

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงานฉบับนี้ เป็นเอกสารอธิบายคำศัพท์ กระบวนการการประเมินความเสี่ยง และการกำหนดระดับความน่าเชื่อถือที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อให้ผู้ที่เกี่ยวข้องกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความเข้าใจตรงกัน

สารบัญ

สารบัญรูป

สารบัญตาราง

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้อธิบายคำศัพท์ กระบวนการ การประเมินความเสี่ยง และการกำหนดระดับความน่าเชื่อถือที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อให้ผู้ที่เกี่ยวข้องกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความเข้าใจตรงกัน

2. บทนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 การพิสูจน์และยืนยันตัวตน หมายถึง กระบวนการพิสูจน์และยืนยันความถูกต้องของตัวบุคคล [1]

2.2 อัตลักษณ์ (identity) หมายถึง ลักษณะเฉพาะของบุคคลซึ่งสามารถบ่งบอกหรือจำแนกได้โดยคุณลักษณะหรือชุดของคุณลักษณะที่เกี่ยวข้องกับตัวบุคคลนั้น [2]

หมายเหตุ 1: ตัวอย่างของคุณลักษณะที่เกี่ยวข้องกับบุคคลธรรมดา เช่น เลขประจำตัว ชื่อบุคคล ที่อยู่ วันเดือนปีเกิด อีเมล หมายเลขโทรศัพท์เคลื่อนที่ ภาพใบหน้า หรือข้อมูลระบุอุปกรณ์ที่บุคคลใช้งาน

หมายเหตุ 2: ตัวอย่างของคุณลักษณะที่เกี่ยวข้องกับนิติบุคคล เช่น เลขทะเบียนนิติบุคคล ชื่อนิติบุคคล ที่ตั้งสำนักงานใหญ่ หรือชื่อกรรมการของนิติบุคคล

2.3 หลักฐานแสดงตน (identity evidence) หมายถึง เอกสารทางกายภาพหรือข้อมูลอิเล็กทรอนิกส์ ซึ่งสามารถใช้เป็นหลักฐานในการพิสูจน์ตัวตน

2.4 การพิสูจน์ตัวตน (identity proofing) หมายถึง กระบวนการรวบรวมและตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคล และการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์นั้น [2]

2.5 สิ่งที่ใช้ยืนยันตัวตน (authenticator) หมายถึง สิ่งที่ใช้เชื่อมโยงอัตลักษณ์กับบุคคล ซึ่งบุคคลนั้นครอบครองและควบคุมเพื่อใช้ในการยืนยันตัวตน เช่น รหัสผ่าน ข้อมูลชีวภาพ [2]

2.6 การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน หมายถึง กระบวนการเชื่อมโยงอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้ยืนยันตัวตน และการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนนั้น [2]

2.7 การยืนยันตัวตน (authentication) หมายถึง กระบวนการยืนยันอัตลักษณ์ของบุคคลด้วยการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้น [2]

2.8 ผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) หมายถึง หน่วยงานที่ให้บริการแก่บุคคลภายนอกเกี่ยวกับการพิสูจน์ตัวตน การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน หรือการยืนยันตัวตน ทั้งนี้ ผู้พิสูจน์และยืนยัน

ตัวตนอาจมอบหมายงานบางส่วนให้ผู้ให้บริการภายนอก (outsourcing) หรือตัวแทนของผู้พิสูจน์และยืนยันตัวตน (agent) โดยผู้พิสูจน์และยืนยันตัวตนรับผิดชอบเสมือนเป็นผู้ดำเนินการเอง

2.9 ผู้อาศัยการยืนยันตัวตน (relying party: RP) หมายถึง บุคคลหรือหน่วยงานที่พึ่งพาอาศัยผลการยืนยันตัวตนจาก IdP หรือสิ่งที่ใช้ยืนยันตัวตนที่ผู้ใช้บริการมีอยู่ก่อนแล้ว ในการตัดสินใจที่จะให้บริการธุรกรรมหรือให้สิทธิในการเข้าใช้งานระบบ

2.10 แหล่งข้อมูลที่น่าเชื่อถือ (authoritative source: AS) หมายถึง แหล่งข้อมูลที่มีการให้ข้อมูลหรือจัดทำข้อมูลอย่างมีเหตุผล มีหลักเกณฑ์ หรือมีการอ้างอิง เพื่อให้ประชาชนหรือกลุ่มธุรกิจสามารถตรวจสอบหรือทราบข้อมูลต่าง ๆ ได้

หมายเหตุ: ตัวอย่างของแหล่งข้อมูลที่น่าเชื่อถือ เช่น ระบบตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยหน่วยงานของรัฐ

2.11 ผู้ใช้บริการ (subscriber) หมายถึง บุคคลที่ผ่านการพิสูจน์ตัวตนและได้รับสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ในการยืนยันตัวตน

2.12 ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL) หมายถึง ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของบุคคล

2.13 ระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL) หมายถึง ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตน

3. การพิสูจน์และยืนยันตัวตนทางดิจิทัล

3.1 ภาพรวม

อัตลักษณ์ (identity) คือ ลักษณะเฉพาะของบุคคลซึ่งสามารถบ่งบอกหรือจำแนกได้โดยคุณลักษณะหรือชุดของคุณลักษณะที่เกี่ยวข้องกับตัวบุคคลนั้น ในขณะที่ดิจิทัลไอดี (digital identity) จะเป็นอัตลักษณ์ที่บันทึกในรูปแบบอิเล็กทรอนิกส์ ซึ่งบุคคลสามารถนำดิจิทัลไอดีไปใช้ในการทำธุรกรรมทางอิเล็กทรอนิกส์ ทั้งนี้ดิจิทัลไอดีของแต่ละบุคคลจะต้องมีความเฉพาะเจาะจงในบริบทของบริการธุรกรรมหนึ่ง ๆ แต่อาจไม่จำเป็นต้องมีความเฉพาะเจาะจงในทุกบริบท อย่างไรก็ตาม บริการธุรกรรมบางประเภทอาจไม่มีความเข้มงวดในการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการ เช่น การให้บริการอีเมลหรือสื่อสังคมออนไลน์ ขณะที่บริการธุรกรรมประเภทที่มีความเสี่ยงสูง เช่น การให้บริการทางการเงิน ผู้ให้บริการจะต้องทราบข้อมูลเกี่ยวกับอัตลักษณ์ที่แท้จริงของผู้ใช้บริการสำหรับใช้เป็นดิจิทัลไอดีในการทำธุรกรรมทางอิเล็กทรอนิกส์

การพิสูจน์ตัวตน (identity proofing) เป็นกระบวนการที่ผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) รวบรวมและตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคล และตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์นั้น โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าอัตลักษณ์ที่กล่าวอ้างเป็นอัตลักษณ์ของบุคคลนั้นจริง (เช่น บุคคลที่กล่าวอ้างว่าตนเองชื่อ “สมชาย” คือ “สมชาย” ตัวจริง ไม่ใช่บุคคลอื่นปลอมตัวมา) ทั้งนี้ข้อเสนอแนะมาตรฐานฉบับนี้กำหนดความเข้มงวดของกระบวนการพิสูจน์ตัวตนเป็นระดับที่เรียกว่า “ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)”

บุคคลที่ผ่านการพิสูจน์ตัวตนเรียบร้อยแล้วจะเปลี่ยนสถานะเป็น “ผู้ใช้บริการ (subscriber)” และได้รับสิ่งที่ใช้ยืนยันตัวตน (authenticator) เพื่อใช้ในการยืนยันอัตลักษณ์ของบุคคล เมื่อผู้ใช้บริการ

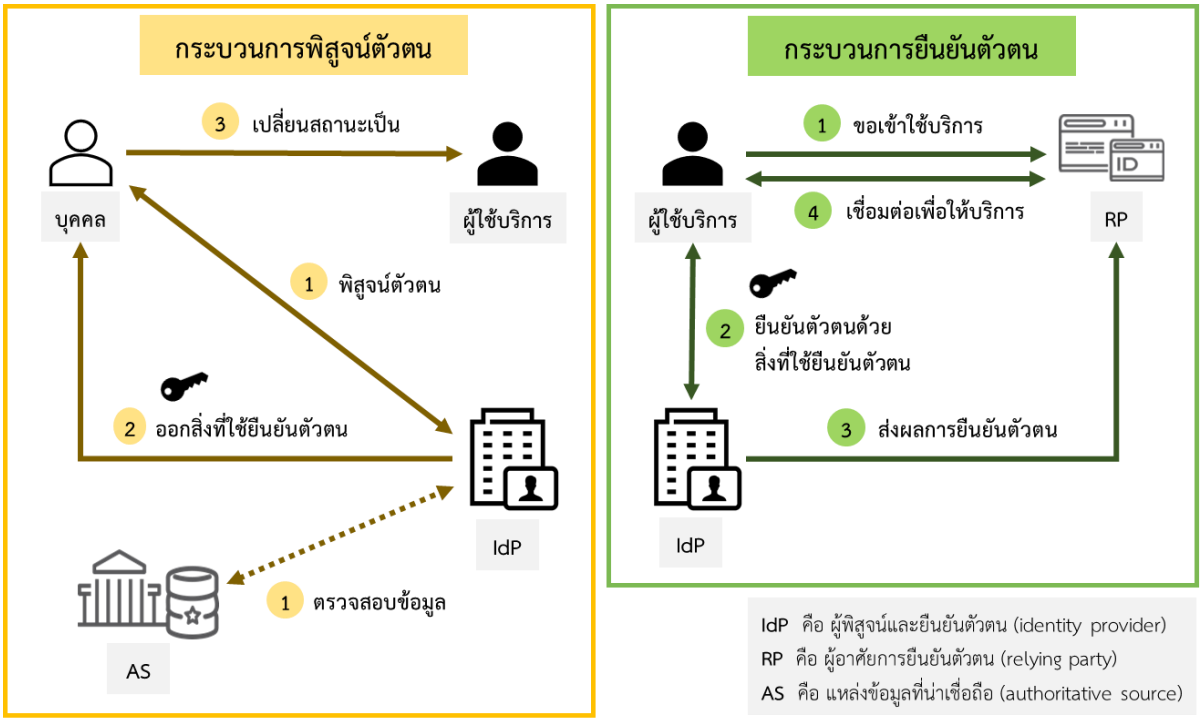
ต้องการเข้าใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์กับผู้อาศัยการยืนยันตัวตน (relying party: RP) ซึ่งเป็นผู้ให้บริการที่ต้องการทราบข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการก่อนตัดสินใจที่จะให้บริการธุรกรรมดังกล่าว RP จะขอให้ IdP ที่ผู้ใช้บริการเคยผ่านการพิสูจน์ตัวตนและได้รับสิ่งที่ใช้ยืนยันตัวตนมาก่อน ช่วยดำเนินการยืนยันตัวตนของผู้ใช้บริการ

การยืนยันตัวตน (authentication) เป็นกระบวนการยืนยันอัตลักษณ์ของบุคคลด้วยการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้น โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าบุคคลที่กำลังเข้าใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนนั้นจริง (เช่น บุคคลที่กำลังเข้าใช้บริการ คือ “สมชาย” ตัวจริง ที่กรอกรหัสผ่านถูกต้อง) ทั้งนี้ ข้อเสนอแนะมาตรฐานฉบับนี้กำหนดความเข้มงวดของกระบวนการยืนยันตัวตนเป็นระดับที่เรียกว่า “ระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL)”

เมื่อผู้ใช้บริการสามารถยืนยันตัวตนกับ IdP ได้ว่าตนเองครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนจริงตามเกณฑ์วิธี (protocol) ที่กำหนด IdP จะส่งผลการยืนยันตัวตน (assertion) ให้กับ RP เพื่อใช้ในการตัดสินใจที่จะให้บริการธุรกรรมหรือให้สิทธิในการเข้าใช้งานระบบ โดยผลการยืนยันตัวตนอาจประกอบด้วยผลการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน และข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการ เช่น เลขประจำตัว ชื่อบุคคล วันเดือนปีเกิด ที่อยู่อีเมล หมายเลขโทรศัพท์เคลื่อนที่ หรือคุณลักษณะอื่น ๆ ที่รวบรวมไว้ในกระบวนการพิสูจน์ตัวตน ซึ่งขึ้นอยู่กับนโยบายของ IdP ความต้องการของ RP และความยินยอมในการเปิดเผยข้อมูลของเจ้าของข้อมูล

3.2 ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้อง

ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้องในการพิสูจน์ตัวตนและยืนยันตัวตน แสดงเป็นแผนภาพตามรูปที่ 1 โดยด้านซ้ายของรูปจะเป็นกระบวนการพิสูจน์ตัวตน และด้านขวาของรูปจะเป็นกระบวนการยืนยันตัวตน



รูปที่ 1 ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้องในการพิสูจน์ตัวตนและยืนยันตัวตน

กระบวนการพิสูจน์ตัวตนมีขั้นตอนทั่วไป ดังนี้

(1) บุคคลที่ประสงค์จะมีดิจิทัลไอดีสำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์มาแสดงตนกับ IdP ซึ่ง IdP จะพิสูจน์ตัวตนของบุคคลตามระดับ IAL ที่กำหนด โดยอาจมีการตรวจสอบหลักฐานแสดงตนและข้อมูลเกี่ยวกับอัตลักษณ์กับ AS รวมถึงการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์นั้น

(2) หากการพิสูจน์ตัวตนสำเร็จ IdP จะออกหรือลงทะเบียนสิ่งที่ใช้ยืนยันตัวตน และเชื่อมโยงอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้ยืนยันตัวตนนั้น โดย IdP มีหน้าที่เก็บรักษาข้อมูลเกี่ยวกับอัตลักษณ์ ข้อมูลการเชื่อมโยงอัตลักษณ์กับสิ่งที่ใช้ยืนยันตัวตน และสถานะของสิ่งที่ใช้ยืนยันตัวตน ตลอดอายุการใช้งานของสิ่งที่ใช้ยืนยันตัวตน

(3) บุคคลที่ผ่านการพิสูจน์ตัวตนแล้วจะเปลี่ยนสถานะเป็นผู้ใช้บริการ และมีหน้าที่ดูแลรักษาสิ่งที่ใช้ยืนยันตัวตนของตนเอง

กระบวนการยืนยันตัวตนซึ่งเกิดขึ้นเมื่อผู้ใช้บริการต้องการเข้าใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์กับ RP มีขั้นตอนทั่วไป ดังนี้

(1) ผู้ใช้บริการขอเข้าใช้บริการหรือทำธุรกรรมกับ RP โดยใช้ดิจิทัลไอดีที่มีระดับ IAL และ AAL สอดคล้องตามความต้องการของ RP

(2) RP นำทาง (redirect) หรือแนะนำให้ผู้ใช้บริการไปยืนยันตัวตนกับ IdP ที่ผู้ใช้บริการเคยผ่านการพิสูจน์ตัวตนมาก่อน และให้ผู้ใช้บริการยืนยันตัวตนกับ IdP ว่าตนเองครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนตามเกณฑ์วิธีหรือระดับ AAL ที่กำหนด

(3) IdP ตรวจสอบความถูกต้องและสถานะของสิ่งที่ใช้ยืนยันตัวตน แล้วส่งผลการยืนยันตัวตนให้กับ RP ซึ่ง RP สามารถใช้ข้อมูลจากผลการยืนยันตัวตนในการตัดสินใจที่จะให้บริการธุรกรรมหรือให้สิทธิในการเข้าใช้งานระบบกับผู้ใช้บริการ

(4) RP ทำการเชื่อมต่อกับผู้ใช้บริการเพื่อให้บริการธุรกรรมหรือให้เข้าใช้งานระบบ

ทั้งนี้ RP และ IdP อาจเป็นหน่วยงานเดียวกัน (กรณีที่ IdP ออกสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ภายในกิจการของหน่วยงาน) หรือเป็นคนละหน่วยงานกัน (กรณีที่ IdP ออกสิ่งที่ใช้ยืนยันตัวตนเพื่อให้บริการแก่บุคคลภายนอก)

3.3 สิ่งที่ใช้ยืนยันตัวตน

สิ่งที่ใช้ยืนยันตัวตน (authenticator) คือ สิ่งที่ใช้เชื่อมโยงอัตลักษณ์กับบุคคล ซึ่งบุคคลนั้นครอบครองและควบคุม เพื่อใช้ในการยืนยันตัวตนกับ IdP ทั้งนี้ สิ่งที่ใช้ยืนยันตัวตนทุกอันจะมีปัจจัยของการยืนยันตัวตน (authentication factor) อย่างน้อยหนึ่งปัจจัย โดยปัจจัยของการยืนยันตัวตนแบ่งออกเป็น 3 ประเภท ดังนี้

(1) สิ่งที่คุณรู้ (something you know) คือ ข้อมูลที่ผู้ใช้บริการเท่านั้นที่ทราบ เช่น รหัสผ่าน (password) และเลขรหัสส่วนตัว (PIN)

(2) สิ่งที่คุณมี (something you have) คือ สิ่งของที่ผู้ใช้บริการเท่านั้นครอบครอง เช่น กุญแจเข้ารหัส (cryptographic key) อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device) และอุปกรณ์ OTP (OTP device)

(3) สิ่งที่คุณเป็น (something you are) คือ ข้อมูลชีวมิติ (biometric data) ของผู้ใช้บริการ เช่น ภาพใบหน้า และลายนิ้วมือ

สิ่งที่ใช้ยืนยันตัวตนอาจประกอบด้วยปัจจัยของการยืนยันตัวตนเพียงหนึ่งปัจจัย (การยืนยันตัวตนแบบปัจจัยเดียว: single-factor authentication) หรือประกอบด้วยปัจจัยของการยืนยันตัวตนมากกว่าหนึ่งปัจจัย (การยืนยันตัวตนแบบหลายปัจจัย: multi-factor authentication) โดยความเข้มงวดของระบบการยืนยันตัวตนจะขึ้นอยู่กับจำนวนปัจจัยของการยืนยันตัวตนและความสามารถในการป้องกันการโจมตีของระบบการยืนยันตัวตน อย่างไรก็ตาม IdP หรือ RP อาจใช้ข้อมูลประกอบอื่น ๆ เช่น ข้อมูลระบุตำแหน่ง หรือข้อมูลระบุอุปกรณ์ที่บุคคลใช้งาน เพื่อเพิ่มความมั่นคงปลอดภัยของระบบการยืนยันตัวตน แต่ข้อมูลเหล่านี้จะไม่ถือเป็นปัจจัยของการยืนยันตัวตน

ในการยืนยันตัวตนแบบไม่พบเห็นต่อหน้า ผู้ใช้บริการต้องแสดงให้เห็นว่าตนเองครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนที่ได้ลงทะเบียนไว้กับ IdP เพื่อยืนยันว่าตนเองเป็นเจ้าของอัตลักษณ์ที่กล่าวอ้างจริง เนื่องจากสิ่งที่ใช้ยืนยันตัวตนจะมีข้อมูลลับ (secret) ที่เฉพาะผู้ใช้บริการตัวจริงเท่านั้นสามารถนำมาใช้ยืนยันตัวตนได้ ทั้งนี้ ข้อมูลลับในสิ่งที่ใช้ยืนยันตัวตนสามารถเป็นคู่กุญแจอสมมาตร (asymmetric keys) หรือข้อมูลลับใช้ร่วมกัน (shared secret)

กรณีที่ข้อมูลลับเป็นคู่กุญแจอสมมาตรซึ่งประกอบด้วยกุญแจส่วนตัว (private key) และกุญแจสาธารณะ (public key) ที่สัมพันธ์กัน ผู้ใช้บริการจะใช้กุญแจส่วนตัวในสิ่งที่ใช้ยืนยันตัวตนเพื่อยืนยันตัวตน ส่วน IdP จะใช้กุญแจสาธารณะที่สัมพันธ์กับกุญแจส่วนตัวเพื่อยืนยันว่าผู้ใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนที่มีกุญแจส่วนตัวนั้น (โดยทั่วไปกุญแจสาธารณะจะอยู่ในรูปแบบใบรับรองกุญแจสาธารณะ (public key certificate))

กรณีที่ข้อมูลลับเป็นข้อมูลลับใช้ร่วมกัน ข้อมูลลับในสิ่งที่ใช้ยืนยันตัวตนอาจเป็นกุญแจสมมาตร (symmetric keys) หรือรหัสลับจดจำ (memorized secret) โดยข้อแตกต่าง คือ กุญแจสมมาตรถูกเลือกจากระบบสุ่มและเก็บไว้ในฮาร์ดแวร์หรือซอฟต์แวร์ที่อยู่ภายใต้การควบคุมของผู้ใช้บริการ ขณะที่รหัสลับจดจำเป็นข้อมูลลับที่ให้ผู้ใช้บริการจดจำ ซึ่งโดยทั่วไป กุญแจเข้ารหัสไม่ว่าจะเป็นกุญแจสมมาตรหรือกุญแจส่วนตัวมักจะมีความยาวของอักขระมากกว่ารหัสลับจดจำ จึงทำให้มีความซับซ้อนที่ยากแก่การคาดเดาโดยผู้ไม่ประสงค์ดี

หมายเหตุ: หลักฐานแสดงตน เช่น บัตรประจำตัวประชาชนหรือใบขับขี่ (ปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี) ซึ่งไม่มีข้อมูลลับในรูปแบบอิเล็กทรอนิกส์ แม้ว่าจะสามารถนำมาใช้ยืนยันตัวตนแบบพบเห็นต่อหน้ากับบุคคล (เช่น เจ้าหน้าที่รักษาความปลอดภัย) แต่ไม่สามารถนำมาใช้ยืนยันตัวตนแบบไม่พบเห็นต่อหน้าได้ เนื่องจากระบบคอมพิวเตอร์ไม่มีข้อมูลให้ตรวจสอบหรือยืนยันตัวตนของผู้ใช้บริการได้

การยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) ซึ่งมีการใช้ปัจจัยของการยืนยันตัวตนมากกว่าหนึ่งปัจจัย สามารถทำได้ 2 วิธี ดังนี้

(1) การใช้ปัจจัยของการยืนยันตัวตนมากกว่าหนึ่งปัจจัยเพื่อยืนยันตัวตนกับ IdP โดยตรง เช่น ผู้ใช้บริการต้องกรอกทั้งรหัสผ่าน (สิ่งที่คุณรู้) และข้อมูลลับที่ส่งมายังโทรศัพท์เคลื่อนที่ของผู้ใช้บริการทาง SMS (สิ่งที่คุณมี) เพื่อยืนยันตัวตนกับ IdP

(2) การใช้ปัจจัยของการยืนยันตัวตนบางปัจจัยเพื่อปกป้องข้อมูลลับก่อนที่จะใช้ยืนยันตัวตนกับ IdP เช่น การใช้ลายนิ้วมือ (สิ่งที่คุณเป็น) เพื่อปกป้องกุญแจส่วนตัว (สิ่งที่คุณมี) ในโทรศัพท์เคลื่อนที่

โดยผู้ใช้บริการต้องสแกนลายนิ้วมือเพื่อทำให้ซอฟต์แวร์เข้ารหัสลับ (cryptographic software) ในโทรศัพท์เคลื่อนที่สามารถเรียกใช้กุญแจส่วนตัวเพื่อยืนยันตัวตนกับ IdP

3.4 ผลการยืนยันตัวตน

หากการยืนยันตัวตนสำเร็จ IdP จะส่งผลการยืนยันตัวตน (assertion) ให้กับ RP โดยผลการยืนยันตัวตนอาจประกอบด้วยผลการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน และข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการ ทั้งนี้ IdP อาจส่งผลการยืนยันตัวตนไปยัง RP โดยตรงผ่านช่องทางที่มั่นคงปลอดภัยเพื่อรักษาความครบถ้วน (integrity) ของผลการยืนยันตัวตน หรืออาจส่งผลการยืนยันตัวตนไปยัง RP ผ่านผู้ใช้บริการ ซึ่ง IdP ต้องจัดให้มีวิธีการรักษาความครบถ้วนของผลการยืนยันตัวตนเพื่อไม่ให้มีการเปลี่ยนแปลงแก้ไขในภายหลัง

RP จะเชื่อถือผลการยืนยันตัวตนหรือไม่ขึ้นอยู่กับแหล่งที่มา เวลาที่สร้าง และสถานะปัจจุบันของผลการยืนยันตัวตน รวมถึงนโยบายของ RP และ IdP ที่เกี่ยวข้องกับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตน นอกจากนี้ RP ต้องตรวจสอบแหล่งที่มา (IdP) และการรักษาความครบถ้วนของผลการยืนยันตัวตน เพื่อให้มั่นใจว่าผลการยืนยันตัวตนไม่ถูกเปลี่ยนแปลงแก้ไขระหว่างการส่งมาจาก IdP ก่อนที่ RP จะนำผลการยืนยันตัวตนไปใช้ในการตัดสินใจต่อไป

หากมีการส่งผลการยืนยันตัวตนผ่านช่องทางที่เป็นเครือข่ายสาธารณะ (public network) IdP ต้องมีวิธีการรักษาความลับ (confidentiality) ของข้อมูลส่วนบุคคลของผู้ใช้บริการที่อยู่ในผลการยืนยันตัวตน เพื่อให้มั่นใจว่าเฉพาะ RP ที่กำหนดเท่านั้นสามารถเข้าถึงข้อมูลได้

3.5 ดิจิทัลไอดีแบบ Federated Identity

ดิจิทัลไอดีแบบ federated identity เป็นรูปแบบการใช้งานดิจิทัลไอดีที่ผู้ใช้บริการสามารถให้ IdP ส่งผลการยืนยันตัวตนเกี่ยวกับผู้ใช้บริการให้กับ RP ที่เป็นคนละระบบหรือคนละหน่วยงานได้ รวมถึง RP อาจพึ่งพาอาศัยผลการยืนยันตัวตนจาก IdP มากกว่าหนึ่งรายก็ได้ โดย IdP และ RP สามารถเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกันผ่านเครือข่ายหรือระบบกลางที่ช่วยอำนวยความสะดวกด้านเทคนิคในการเชื่อมต่อและตั้งค่าระบบของ IdP RP และผู้ที่เกี่ยวข้องอื่น ๆ

การใช้งานดิจิทัลไอดีแบบ federated identity มีประโยชน์หลายอย่าง เช่น

(1) เพิ่มความสะดวกให้กับผู้ใช้บริการ โดยผู้ใช้บริการสามารถพิสูจน์ตัวตนกับ IdP รายใดรายหนึ่ง และนำสิ่งที่ใช้ยืนยันตัวตนที่ได้รับจาก IdP นั้นมาใช้ยืนยันตัวตนเพื่อเข้าใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์กับ RP หลายรายได้

(2) ลดค่าใช้จ่ายให้กับ RP ในการพัฒนาโครงสร้างพื้นฐานทางเทคโนโลยี (เช่น การจัดการบัญชีผู้ใช้งานและสิ่งที่ใช้ยืนยันตัวตน) และลดภาระของผู้ใช้บริการในการครอบครองหรือเก็บรักษาสิ่งที่ใช้ยืนยันตัวตนที่แตกต่างกันของ RP แต่ละราย เนื่องจาก RP ในกลุ่มเดียวกันสามารถอาศัยสิ่งที่ใช้ยืนยันตัวตนหรือข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการร่วมกันได้

(3) ทำให้หน่วยงานสามารถมุ่งเน้นการดำเนินงานไปที่ภารกิจหลักของหน่วยงานโดยตรง แทนที่การดำเนินงานด้านการพิสูจน์และยืนยันตัวตน

4. การกำหนดระดับความน่าเชื่อถือ

4.1 ภาพรวม

ความเสี่ยงที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนตามข้อเสนอแนะมาตรฐานฉบับนี้ แบ่งออกเป็น 2 ด้าน คือ ความเสี่ยงของการพิสูจน์ตัวตนที่ผิดพลาด (เช่น บุคคลที่มาพิสูจน์ตัวตนแอบอ้างอัตลักษณ์ของบุคคลอื่นหรือใช้หลักฐานแสดงตนปลอม) และความเสี่ยงของการยืนยันตัวตนที่ผิดพลาด (เช่น บุคคลที่แสดงสิ่งที่ใช้ยืนยันตัวตนไม่ใช่เจ้าของสิ่งที่ใช้ยืนยันตัวตนจริง) โดยผลกระทบที่อาจเกิดขึ้นจากความผิดพลาดของการพิสูจน์และยืนยันตัวตน คือ การให้บริการธุรกรรมหรือให้สิทธิในการเข้าใช้งานระบบแก่บุคคลที่ไม่ถูกต้อง

ด้วยเหตุนี้ ผู้ให้บริการจึงต้องประเมินความเสี่ยงของการพิสูจน์ตัวตนที่ผิดพลาดและการยืนยันตัวตนที่ผิดพลาด เพื่อให้สามารถกำหนดระดับความน่าเชื่อถือที่เหมาะสมกับแต่ละบริการธุรกรรม และกำหนดกระบวนการและเทคโนโลยีที่จะใช้ให้เป็นไปตามระดับความน่าเชื่อถือแต่ละระดับ

4.2 ระดับความน่าเชื่อถือ

ผู้ให้บริการควรกำหนดระดับความน่าเชื่อถือ (assurance level) ของการพิสูจน์ตัวตนและการยืนยันตัวตนสำหรับแต่ละบริการธุรกรรมตามความเสี่ยงของบริการธุรกรรมนั้น ข้อเสนอแนะมาตรฐานฉบับนี้แบ่งระดับความน่าเชื่อถือเป็น 2 ด้าน ดังนี้

(1) ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน คือ ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของบุคคล การกำหนดระดับ IAL ที่เหมาะสมจะช่วยลดโอกาสของการพิสูจน์ตัวตนที่ผิดพลาด โดยระดับ IAL แบ่งออกเป็น 3 ระดับ คือ IAL1 (ความน่าเชื่อถือต่ำที่สุด) IAL2 และ IAL3 (ความน่าเชื่อถือสูงที่สุด)

รายละเอียดเป็นไปตามข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน (เวอร์ชัน 3.0)

(2) ระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL)

ระดับความน่าเชื่อถือของการยืนยันตัวตน คือ ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตน การกำหนดระดับ AAL ที่เหมาะสมจะช่วยลดโอกาสของการยืนยันตัวตนที่ผิดพลาด โดยระดับ AAL แบ่งออกเป็น 3 ระดับ คือ AAL1 (ความน่าเชื่อถือต่ำที่สุด) AAL2 และ AAL3 (ความน่าเชื่อถือสูงที่สุด)

รายละเอียดเป็นไปตามข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการยืนยันตัวตน (เวอร์ชัน 3.0)

4.3 การประเมินความเสี่ยงเพื่อกำหนดระดับความน่าเชื่อถือ

การประเมินความเสี่ยงเพื่อกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) ให้เหมาะสมกับแต่ละบริการธุรกรรม ประกอบด้วย 2 ขั้นตอน คือ (1) การประเมินระดับผลกระทบที่เป็นไปได้ และ (2) การเชื่อมโยงระดับผลกระทบที่เป็นไปได้เข้ากับระดับความน่าเชื่อถือ โดยมีรายละเอียดดังนี้

(1) ขั้นตอนที่ 1: การประเมินระดับผลกระทบที่เป็นไปได้

การประเมินระดับผลกระทบที่เป็นไปได้ (potential impact) เป็นการพิจารณาผลกระทบที่เป็นไปได้จากการพิสูจน์ตัวตนที่ผิดพลาด (สำหรับการกำหนดระดับ IAL) และผลกระทบที่เป็นไปได้จากการยืนยันตัวตนที่ผิดพลาด (สำหรับการกำหนดระดับ AAL)

ผู้ให้บริการควรประเมินความเสี่ยงและผลกระทบที่เป็นไปได้ของบริการธุรกรรม โดยพิจารณาให้เป็นไปตามหลักเกณฑ์ของหน่วยงานที่กำกับดูแลบริการธุรกรรมแต่ละประเภท นโยบายการบริหารความเสี่ยงของหน่วยงานของตนเอง และบริบทการใช้งานของบริการธุรกรรมนั้น อย่างไรก็ตาม ผู้ให้บริการอาจพิจารณาแบ่งประเภทของผลกระทบ (impact category) เป็น 6 ด้าน ดังนี้

- ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง
- ความเสียหายทางการเงิน
- ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ
- การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
- ความปลอดภัยของบุคคล
- การละเมิดทางแพ่งหรือทางอาญา

การประเมินระดับผลกระทบที่เป็นไปได้จะใช้วิธีการพิจารณาระดับผลกระทบแต่ละด้านที่สามารถเป็นไปได้เมื่อเกิดข้อผิดพลาด ตามตารางที่ 1

ตารางที่ 1 เกณฑ์การประเมินระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด

ด้านของผลกระทบ	ระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด		
	ต่ำ	ปานกลาง	สูง
ความไม่สะดวกสบายและเสื่อมเสียชื่อเสียง	มีความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียงในระยะสั้นและจำกัด	มีความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียงรุนแรงระยะสั้น หรือมีผลปานกลางในระยะยาว	มีความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียงระยะยาว หรือมีผลกระทบหลายบุคคล
ความเสียหายทางการเงิน	มีความเสียหายทางการเงินที่ไม่มีนัยสำคัญ	มีความเสียหายทางการเงินรุนแรง	มีความเสียหายทางการเงินรุนแรงมาก
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบที่จำกัดต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงมากต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	มีการปล่อยข้อมูลส่วนบุคคลหรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับต่ำ	มีการปล่อยข้อมูลส่วนบุคคลหรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับปานกลาง	มีการปล่อยข้อมูลส่วนบุคคลหรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับสูง

ด้านของผลกระทบ	ระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด		
	ต่ำ	ปานกลาง	สูง
ความปลอดภัยของบุคคล	บาดเจ็บเล็กน้อย ไม่ต้องรับการรักษาพยาบาล	มีความเสี่ยงพอสมควรที่จะบาดเจ็บเล็กน้อย หรือมีความเสี่ยงจำกัดที่จะบาดเจ็บซึ่งต้องรับการรักษาพยาบาล	มีความเสี่ยงที่จะบาดเจ็บสาหัส หรือถึงแก่ชีวิต
การละเมิดทางแพ่งหรือทางอาญา	การฝ่าฝืนกฎหมายนั้นเป็นเรื่องเล็กน้อย ซึ่งไม่จำเป็นต้องมีการบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงที่จะถูกบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงสูงที่จะถูกบังคับใช้กฎหมาย

(2) ขั้นตอนที่ 2: การเชื่อมโยงระดับผลกระทบที่เป็นไปได้เข้ากับระดับความน่าเชื่อถือ

ผลการประเมินระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาดในการพิสูจน์ตัวตนและการยืนยันตัวตนจากขั้นตอนที่ 1 จะนำมาเชื่อมโยงเข้ากับระดับความน่าเชื่อถือ IAL และ AAL ตามลำดับ โดยระดับความน่าเชื่อถือ IAL และ AAL ที่เหมาะสมคือระดับที่ครอบคลุมผลกระทบที่เป็นไปได้ทุกด้านตามตารางที่ 2

ตารางที่ 2 ระดับผลกระทบที่เป็นไปได้และระดับความน่าเชื่อถือที่ต้องการ

ด้านของผลกระทบ	ระดับความน่าเชื่อถือที่ต้องการ		
	1	2	3
ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง	ต่ำ	ปานกลาง	สูง
ความเสียหายทางการเงิน	ต่ำ	ปานกลาง	สูง
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	ไม่มี	ต่ำ/ปานกลาง	สูง
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	ไม่มี	ต่ำ/ปานกลาง	สูง
ความปลอดภัยของบุคคล	ไม่มี	ต่ำ	ปานกลาง/สูง
การละเมิดทางแพ่งหรือทางอาญา	ไม่มี	ต่ำ/ปานกลาง	สูง

4.4 ตัวอย่างการกำหนดระดับความน่าเชื่อถือ

ตัวอย่างการกำหนดระดับความน่าเชื่อถือ IAL และ AAL ของ RP มีขั้นตอนดังนี้

(1) การกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL)

(1.1) ขั้นตอนที่ 1: การประเมินระดับผลกระทบที่เป็นไปได้จากการพิสูจน์ตัวตนที่ผิดพลาด โดยมีตัวอย่างของผลการประเมิน ดังนี้

ด้านของผลกระทบ	ระดับผลกระทบ
ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง	ต่ำ
ความเสียหายทางการเงิน	ต่ำ
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	ไม่มี
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	ไม่มี
ความปลอดภัยของบุคคล	ไม่มี
การละเมิดทางแพ่งหรือทางอาญา	ไม่มี

(1.2) ขั้นตอนที่ 2: การเชื่อมโยงผลระดับผลกระทบที่เป็นไปได้เข้ากับระดับความน่าเชื่อถือ

ด้านของผลกระทบ	ระดับความน่าเชื่อถือที่ต้องการ		
	1	2	3
ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง	ต่ำ	ปานกลาง	สูง
ความเสียหายทางการเงิน	ต่ำ	ปานกลาง	สูง
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	ไม่มี	ต่ำ/ปานกลาง	สูง
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	ไม่มี	ต่ำ/ปานกลาง	สูง
ความปลอดภัยของบุคคล	ไม่มี	ต่ำ	ปานกลาง/สูง
การละเมิดทางแพ่งหรือทางอาญา	ไม่มี	ต่ำ/ปานกลาง	สูง

จากการเชื่อมโยงระดับผลกระทบที่เป็นไปได้ (จากขั้นตอนที่ 1) เข้ากับระดับความน่าเชื่อถือ พบว่า ระดับความน่าเชื่อถือที่ครอบคลุมผลกระทบที่เป็นไปได้ทุกด้าน คือ ระดับ 1 ดังนั้น ระดับความน่าเชื่อถือ IAL ที่เหมาะสมในตัวอย่างนี้ คือ ระดับ IAL1

(2) การกำหนดระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL)

(2.1) ขั้นตอนที่ 1: การประเมินระดับผลกระทบที่เป็นไปได้จากการยืนยันตัวตนที่ผิดพลาด โดยมีตัวอย่างของผลการประเมิน ดังนี้

ด้านของผลกระทบ	ระดับผลกระทบ
ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง	ต่ำ
ความเสียหายทางการเงิน	ต่ำ
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	ต่ำ
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	ปานกลาง
ความปลอดภัยของบุคคล	ไม่มี
การละเมิดทางแพ่งหรือทางอาญา	ต่ำ

(2.2) ขั้นตอนที่ 2: การเชื่อมโยงระดับผลกระทบที่เป็นไปได้เข้ากับระดับความน่าเชื่อถือ

ด้านของผลกระทบ	ระดับความน่าเชื่อถือที่ต้องการ		
	1	2	3
ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง	ต่ำ	ปานกลาง	สูง
ความเสียหายทางการเงิน	ต่ำ	ปานกลาง	สูง
ความเสียหายต่อการดำเนินงานขององค์กร หรือต่อผลประโยชน์สาธารณะ	ไม่มี	ต่ำ/ปานกลาง	สูง
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	ไม่มี	ต่ำ/ปานกลาง	สูง
ความปลอดภัยของบุคคล	ไม่มี	ต่ำ	ปานกลาง/สูง
การละเมิดทางแพ่งหรือทางอาญา	ไม่มี	ต่ำ/ปานกลาง	สูง

จากการเชื่อมโยงระดับผลกระทบที่เป็นไปได้ (จากขั้นตอนที่ 1) เข้ากับระดับความน่าเชื่อถือ พบว่า ระดับความน่าเชื่อถือที่ครอบคลุมผลกระทบที่เป็นไปได้ทุกด้าน คือ ระดับ 2 ดังนั้น ระดับความน่าเชื่อถือ AAL ที่เหมาะสมในตัวอย่างนี้ คือ ระดับ AAL2

ภาคผนวก ก. อักษรย่อ

อักษรย่อ	คำเต็ม	คำภาษาไทย
IdP	identity provider	ผู้พิสูจน์และยืนยันตัวตน
RP	relying party	ผู้อาศัยการยืนยันตัวตน
AS	authoritative source	แหล่งข้อมูลที่น่าเชื่อถือ
IAL	identity assurance level	ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน
AAL	authentication assurance level	ระดับความน่าเชื่อถือของการยืนยันตัวตน
PIN	personal identification number	เลขรหัสส่วนตัว
OTP	one-time password	รหัสผ่านใช้ครั้งเดียว
FMR	false match rate	อัตราการเข้าคู่ผิดพลาด
FNMR	false non-match rate	อัตราการไม่เข้าคู่ผิดพลาด

บรรณานุกรม

[1] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม.

[2] พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. 2565.

[3] National Institute of Standards and Technology, U.S. Department of Commerce, "NIST Special Publication 800-63-3, Digital Identity Guidelines", June 2017.

[4] International Organization for Standardization, "ISO/IEC 29115:2013 Information technology – Security techniques – Entity authentication assurance framework", April 2013.

[5] Digital Transformation Agency, Australian Government, "Trusted Digital Identity Framework (TDIF): 01 - Glossary of Abbreviations and Terms", Release 4.6, March 2022.