ยกเลิกการใช้งานข้อเสนอแนะมาตรฐานฯ ฉบับนี้

ข้อเสนอแนะมาตรฐานฯ ที่ประกาศยกเลิก

เลขที่	ขมธอ. 19-2564 เวอร์ชัน 2.0
ชื่อเอกสาร	การพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน (Digital Identity – Identity Proofing Requirements)
วันที่ประกาศใช้	30 กันยายน พ.ศ. 2564
วันที่ประกาศยกเลิก	23 กุมภาพันธ์ พ.ศ. 2566

ข้อเสนอแนะมาตรฐานฯ ที่ประกาศใช้แทนฉบับเดิม

เลขที่	ขมธอ. 19-2566 เวอร์ชัน 3.0
ชื่อเอกสาร	การพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน (Digital Identity – Identity Proofing Requirements)
วันที่ประกาศใช้	23 กุมภาพันธ์ พ.ศ. 2566

ETDA

ETDA
สพธอ
www.etda.or.th

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard

for Electronic Transactions

ขมธอ. 19-2564

ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน

DIGITAL IDENTITY –
IDENTITY PROOFING REQUIREMENTS

เวอร์ชัน 2.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.030

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน

ขมธอ. 19-2564

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 30 กันยายน พ.ศ. 2564

คณะอนุกรรมการมาตรฐานและการกำกับดูแล
ภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

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 กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ
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

คณะทำงานนำร่องการใช้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

(จัดทำข้อเสนอแนะมาตรฐานฯ เลขที่ ขมธอ. 18-2561 ขมธอ. 19-2561 และ ขมธอ. 20-2561)

ประธานคณะทำงานร่วม

นางสาวสิริธิดา พนมวัน ณ อยุธยา	ธนาคารแห่งประเทศไทย
นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

รองประธานคณะทำงาน

นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงาน

นายอภิวัฒน์ อินขัด	กรมการกงสุล
นายวีนัส สีสุข	กรมการปกครอง
นายสัญชัย เตชนิมิตวัช	
นายสุชาติ ธานีรัตน์	
นายเผด็จ เรือนจันทร์	กรมพัฒนาธุรกิจการค้า
นางสาวขนิษฐา สหเมธาพัฒน์	กรมสรรพากร
นางอารีย์พันธ์ เจริญสุข	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นางสาวนิชา สาทรกิจ	
นางวณิสรา สุขวัฒน์	
นายสุวิจักขณ์ ธรรมชัยพจน์	สำนักงานป้องกันและปราบปรามการฟอกเงิน
นายสรรเพชญ แสงเนตรสว่าง	
นายบัญชา มนูญกุลชัย	ธนาคารแห่งประเทศไทย
นายสุวิทย์ ตันรุ่งเรือง	
นางสาวสาริกา อภิวรรธกกุล	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
นายศุภกิจ สัตยารัฐ	สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
นายอนุชิต ชื่นชมภู	บริษัท ไปรษณีย์ไทย จำกัด
นายณัฐ เลิศฤทธิ์	
นางสาวนันทวัน วงศ์ขจรกิตติ	กองทุนเงินให้กู้ยืมเพื่อการศึกษา
นางวรวรรณ ธาราภูมิ	สมาคมบริษัทจัดการลงทุน
นางสาวยุภาวรรณ ศิริชัยนฤมิตร	ตลาดหลักทรัพย์แห่งประเทศไทย
นายฐานิสร์ ฟอลเล็ต	สมาคมการค้าผู้ให้บริการชำระเงินอิเล็กทรอนิกส์ไทย
นายฐากร ปิยะพันธ์	สมาคมธนาคารไทย
นางสาวสุญาณี ภูริปัญญวานิช	สมาคมธนาคารไทย
นายสุวิชชา สุดใจ	สมาคมธนาคารไทย
นายศีลวัต สันติวิสัฏฐ์	สมาคมธนาคารไทย
นางอภิพันธ์ เจริญอนุสรณ์	สมาคมธนาคารไทย

นางประราลี รัตน์ประสาทพร	สมาคมธนาคารไทย
นางภัทธีรา ดิลกรุ่งธีระภพ	สมาคมบริษัทหลักทรัพย์ไทย
นายพิเชษฐ สิทธิอำนวย	สมาคมบริษัทหลักทรัพย์ไทย
นายญาณศักดิ์ มโนมัยพิบูลย์	สมาคมบริษัทหลักทรัพย์ไทย
นายสุรศักดิ์ กลิ่นศรีสุข	สมาคมประกันชีวิตไทย
นายจรุง เชื้อจินดา	สมาคมประกันชีวิตไทย
นายพีระพัฒน์ เมฆสิงห์วี	สมาคมประกันวินาศภัยไทย
นายชูชัย วชิรบรรจง	สมาคมประกันวินาศภัยไทย

คณะทำงานและเลขานุการร่วม

นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายธนฉัตร วิจารณ์ปรีชา	ธนาคารเกียรตินาคิน จำกัด (มหาชน)

ผู้ช่วยเลขานุการ

นายนครินทร์ ลิ้มรังษี	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตนฉบับนี้ จัดทำขึ้นเพื่อเป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการพิสูจน์ตัวตนของบุคคลที่ประสงค์จะใช้บริการหรือทำธุรกรรมอิเล็กทรอนิกส์ เพื่อให้ IdP มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกันตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)

โดยมีการนำเสนอและรับฟังความคิดเห็นเป็นการทั่วไป ตลอดจนพิจารณาข้อมูล ข้อสังเกต ข้อคิดเห็นจากผู้ทรงคุณวุฒิและจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความสมบูรณ์ครบถ้วนยิ่งขึ้น รวมทั้งให้สามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตนฉบับนี้ 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 สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชนจึงได้ร่วมกันจัดทำมาตรฐานแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย โดยประกาศเป็นข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ (ETDA Recommendation) เมื่อวันที่ 28 กันยายน พ.ศ. 2561 ซึ่งประกอบด้วยข้อเสนอแนะมาตรฐานฯ จำนวน 3 ฉบับ ดังนี้

(1) ข้อเสนอแนะมาตรฐานฯ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ (เวอร์ชัน 1.0) เลขที่ ขมธอ. 18-2561
(2) ข้อเสนอแนะมาตรฐานฯ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน (เวอร์ชัน 1.0) เลขที่ ขมธอ. 19-2561
(3) ข้อเสนอแนะมาตรฐานฯ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน (เวอร์ชัน 1.0) เลขที่ ขมธอ. 20-2561

ต่อมา กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์กำหนดให้บุคคลสามารถพิสูจน์และยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ โดยมีกลไกการควบคุมดูแลผู้ประกอบธุรกิจบริการที่เกี่ยวข้องเพื่อให้ระบบดังกล่าวมีความน่าเชื่อถือและปลอดภัย ป้องกันความเสียหายที่อาจเกิดขึ้นต่อสาธารณชน ตลอดจนเสริมสร้างความน่าเชื่อถือและการยอมรับในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ในการนี้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์จึงได้แก้ไขปรับปรุงข้อเสนอแนะมาตรฐานฯ ฉบับเดิม เพื่อให้แนวทางการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความสอดคล้องกับบริบทการใช้งาน ความต้องการทางธุรกิจและคุณลักษณะของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลในประเทศไทย โดยจัดทำเป็นข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อมาใช้แทนข้อเสนอแนะมาตรฐานฯ ฉบับเดิม และยกเลิกข้อเสนอแนะมาตรฐานฯ ฉบับเดิม (ข้อเสนอแนะมาตรฐานฯ เลขที่ ขมธอ. 18-2561 ขมธอ. 19-2561 และ ขมธอ. 20-2561)

ข้อเสนอแนะมาตรฐานฉบับนี้เป็นส่วนหนึ่งของชุดข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งประกอบด้วย

(1) ข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน (เวอร์ชัน 2.0)
(2) ข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน (เวอร์ชัน 2.0)
(3) ข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการยืนยันตัวตน (เวอร์ชัน 2.0)

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตนฉบับนี้ เป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการพิสูจน์ตัวตนของบุคคลที่ประสงค์จะใช้บริการหรือทำธุรกรรมอิเล็กทรอนิกส์ เพื่อให้ IdP มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกันตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)

สารบัญ

สารบัญตาราง

ETDA
สพธอ
www.etda.or.th

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์
ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน

โดยที่เป็นการสมควรปรับปรุงข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้แนวทางการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความสอดคล้องกับบริบทการใช้งาน ความต้องการทางธุรกิจ และคุณลักษณะของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลในประเทศไทย

อาศัยอำนาจตามความในมาตรา ๕ แห่งพระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๒ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ จึงให้ยกเลิกประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน เลขที่ ขมธอ. ๑๙-๒๕๖๑ ลงวันที่ ๑๑ กุมภาพันธ์ ๒๕๖๒ และประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน เลขที่ ขมธอ. ๑๙-๒๕๖๔ ปรากฏตามท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๓๐ กันยายน พ.ศ. ๒๕๖๔

ชัยชนะ มิตรพันธ์

(นายชัยชนะ มิตรพันธ์)
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้เป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการพิสูจน์ตัวตนของบุคคลที่ประสงค์จะใช้บริการหรือทำธุรกรรมอิเล็กทรอนิกส์ เพื่อให้ IdP มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกันตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)

ข้อเสนอแนะมาตรฐานฉบับนี้เป็นข้อกำหนดสำหรับหน่วยงานที่ให้บริการพิสูจน์และยืนยันตัวตนแก่บุคคลภายนอก ข้อกำหนดในข้อเสนอแนะมาตรฐานฉบับนี้สามารถประยุกต์ใช้ได้กับบริการพิสูจน์และยืนยันตัวตนที่ใช้เพื่อประโยชน์ภายในกิจการของหน่วยงาน ทั้งนี้ ไม่มีเจตนาปิดกั้นหรือห้ามใช้วิธีการอื่นเพื่อเพิ่มประสิทธิภาพของการพิสูจน์และยืนยันตัวตน

ข้อเสนอแนะมาตรฐานฉบับนี้มีรูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) ดังต่อไปนี้

- “ต้อง” (shall) ใช้ระบุสิ่งที่เป็นข้อกำหนด (requirement) ซึ่งต้องปฏิบัติตาม
- “ควร” (should) ใช้ระบุสิ่งที่เป็นข้อแนะนำ (recommendation)
- “อาจ” (may) ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้ (permission)

2. การพิสูจน์ตัวตน

การพิสูจน์ตัวตน (identity proofing) เป็นกระบวนการที่ IdP รวบรวมและตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ และตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์นั้น โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าอัตลักษณ์ที่กล่าวอ้างเป็นอัตลักษณ์ของบุคคลนั้นจริงตามระดับความน่าเชื่อถือที่กำหนด โดยผลลัพธ์ที่คาดหวังจากการพิสูจน์ตัวตนของบุคคลที่ประสงค์จะมีดิจิทัลไอดีสำหรับการทำธุรกรรมอิเล็กทรอนิกส์ ประกอบด้วย

- สามารถแยกแยะอัตลักษณ์ที่กล่าวอ้างว่าอัตลักษณ์นั้นมีเพียงอันเดียวและมีความเฉพาะเจาะจงภายในบริบทของบริการธุรกรรม
- สามารถตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ว่ามีความถูกต้อง แท้จริง และเป็นปัจจุบัน
- สามารถตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับอัตลักษณ์ที่กล่าวอ้าง

การพิสูจน์ตัวตนประกอบด้วยกระบวนการพื้นฐาน 3 กระบวนการ ดังนี้

2.1 การรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์

การรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ คือ กระบวนการที่ IdP รวบรวมข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตน เพื่อใช้แยกแยะว่าอัตลักษณ์ที่กล่าวอ้างมีเพียงอันเดียวและมีความเฉพาะเจาะจงภายในบริบทของบริการธุรกรรม

2.2 การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์

การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ คือ กระบวนการที่ IdP ตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบันของข้อมูลเกี่ยวกับอัตลักษณ์ เพื่อพิสูจน์ว่าอัตลักษณ์ที่กล่าวอ้างเป็นข้อมูลของบุคคลที่มีอยู่จริง

2.3 การตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์

การตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์ คือ กระบวนการที่ IdP ตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับอัตลักษณ์ที่กล่าวอ้าง เพื่อพิสูจน์ว่าอัตลักษณ์ที่กล่าวอ้างเป็นอัตลักษณ์จริงของบุคคลที่กำลังพิสูจน์ตัวตน

หลังจากพิสูจน์ตัวตนเรียบร้อยแล้ว IdP จะเชื่อมโยงอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้ยืนยันตัวตน (authenticator) โดยบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วจะเปลี่ยนสถานะเป็นผู้ใช้บริการ และได้รับสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ในการยืนยันตัวตนต่อไป

3. ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL)

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL) คือ ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของบุคคล โดยระดับ IAL แบ่งออกเป็น 3 ระดับ ดังนี้

3.1 ระดับ IAL1

ระดับ IAL1 อาจมีการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ ซึ่งเป็นข้อมูลที่บุคคลยืนยันด้วยตนเอง (self-asserted) อย่างไรก็ตาม IAL1 อาจมีการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์หรือการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์ด้วยวิธีการอื่น ๆ ตามความเสี่ยงของบริการธุรกรรม นอกเหนือจากวิธีการที่กำหนดไว้ในระดับ IAL2 และ IAL3 เช่น

- ตรวจสอบสำเนาหรือรูปถ่ายของหลักฐานแสดงตน [1]
- ตรวจสอบลักษณะทางกายภาพของหลักฐานแสดงตนโดยเจ้าหน้าที่
- ตรวจสอบข้อมูลบนหน้าหลักฐานแสดงตนและตรวจสอบสถานะของบัตรประจำตัวประชาชน
- เปรียบเทียบภาพใบหน้าของบุคคลกับภาพใบหน้าบนหน้าหลักฐานแสดงตน
- ยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ (เช่น หมายเลขโทรศัพท์ อีเมล)

[1] กรณีบัตรประจำตัวประชาชนแบบอเนกประสงค์ ควรจัดเก็บสำเนาหรือรูปถ่ายบัตรประจำตัวประชาชนเฉพาะด้านหน้าเพียงด้านเดียวตามคำแนะนำของกระทรวงมหาดไทย [5] ไม่ควรจัดเก็บสำเนาหรือรูปถ่ายด้านหลังบัตรประจำตัวประชาชน เนื่องจากหมายเลขหลังบัตรประจำตัวประชาชน (laser code) เป็นข้อมูลที่อาจใช้ในการยืนยันตัวตนหรือทำธุรกรรมในบางกรณี หากมีการรั่วไหลของข้อมูลดังกล่าว อาจจะทำให้เกิดความเสียหายต่อผู้ใช้บริการ

3.2 ระดับ IAL2

ระดับ IAL2 กำหนดให้มีการขอหลักฐานแสดงตน การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ว่าอัตลักษณ์ที่กล่าวอ้างเป็นข้อมูลของบุคคลที่มีอยู่จริง และการตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับอัตลักษณ์นั้น ทั้งนี้ การพิสูจน์ตัวตนที่ระดับ IAL2 สามารถทำได้ทั้งแบบพบเห็นต่อหน้า (face-to-face) หรือแบบไม่พบเห็นต่อหน้า (non face-to-face) เช่น การพิสูจน์ตัวตนผ่านเครื่องให้บริการ (kiosk) หรือแอปพลิเคชันของ IdP

IdP ที่รองรับระดับ IAL2 สามารถส่งผลการยืนยันตัวตนและข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลนั้นให้กับ RP ที่ต้องการระดับ IAL เท่ากันหรือต่ำกว่าได้ หากได้รับความยินยอมจากบุคคลที่เป็นเจ้าของข้อมูล

ในทางปฏิบัติ ระดับ IAL2 จะแบ่งออกเป็น 3 ระดับย่อย คือ IAL2.1, IAL2.2 และ IAL2.3 โดยพิจารณาจากความเข้มงวดของวิธีการที่ใช้ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์หรือตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์

3.3 ระดับ IAL3

ระดับ IAL3 เพิ่มความเข้มงวดจากระดับ IAL2 โดยกำหนดให้มีการตรวจสอบกับแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติม และการตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับอัตลักษณ์ที่กล่าวอ้างด้วยการเปรียบเทียบข้อมูลชีวมิติ (biometric comparison) เพื่อป้องกันการปลอมตัวเป็นบุคคลอื่นและการลงทะเบียนซ้ำ ทั้งนี้ การพิสูจน์ตัวตนที่ระดับ IAL3 สามารถทำได้แบบพบเห็นต่อหน้า (face-to-face) เท่านั้น

IdP ที่รองรับระดับ IAL3 สามารถส่งผลการยืนยันตัวตนและข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลนั้นให้กับ RP ที่ต้องการระดับ IAL เท่ากันหรือต่ำกว่าได้ หากได้รับความยินยอมจากบุคคลที่เป็นเจ้าของข้อมูล

4. ข้อกำหนดของการพิสูจน์ตัวตน

4.1 ข้อกำหนดของการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์

ข้อกำหนดของการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ตามระดับ IAL สามารถแสดงได้ตามตารางที่ 1

ตารางที่ 1 ข้อกำหนดของการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์

ระดับ IAL	ข้อกำหนดของการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์
IAL1	(1) IdP อาจรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ ซึ่งเป็นข้อมูลที่บุคคลยืนยันด้วยตนเอง (self-asserted) เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจง
IAL2	(1) IdP ต้องรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตนอย่างน้อย 1 ฉบับ เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจง (2) IdP ที่รองรับระดับ IAL2 สามารถส่งข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลให้กับ RP ที่ต้องการระดับ IAL เท่ากันหรือต่ำกว่าได้ หากได้รับความยินยอมจากบุคคลที่เป็นเจ้าของข้อมูล
IAL3	(1) IdP ต้องรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตนอย่างน้อย 1 ฉบับ และรวบรวมข้อมูลจากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติม เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจง

ระดับ IAL	ข้อกำหนดของการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์
	(2) IdP ที่รองรับระดับ IAL3 สามารถส่งข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลให้กับ RP ที่ต้องการระดับ IAL เท่ากันหรือต่ำกว่าได้ หากได้รับความยินยอมจากบุคคลที่เป็นเจ้าของข้อมูล

4.2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์

ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ตามระดับ IAL สามารถแสดงได้ตามตารางที่ 2

ตารางที่ 2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์

ระดับ IAL	ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์
IAL1	IdP ไม่จำเป็นต้องตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์
IAL2.1	<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์เป็นหลักฐานแสดงตน</u> (1) IdP <u>ต้อง</u>ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์จากเครื่องอ่านบัตรประจำตัวประชาชนแบบอเนกประสงค์ (2) กรณีไม่มีเครื่องอ่านบัตรประจำตัวประชาชนแบบอเนกประสงค์ IdP สามารถตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์จากผลการยืนยันตัวตนที่ส่งให้โดย IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 เป็นอย่างน้อย ทั้งนี้ การส่งผลการยืนยันตัวตนที่มีข้อมูลเกี่ยวกับอัตลักษณ์<u>ต้อง</u>ให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย (3) IdP <u>ควร</u>ตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล <u>กรณีใช้หนังสือเดินทางเป็นหลักฐานแสดงตน</u> (1) IdP <u>ต้อง</u>ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์จากเทคโนโลยีสื่อสารไร้สายระยะใกล้ (near field communication: NFC) (2) IdP <u>ควร</u>ตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล
IAL2.2	<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์เป็นหลักฐานแสดงตน</u> (1) IdP <u>ต้องตรวจสอบ</u>ข้อมูลเกี่ยวกับอัตลักษณ์จากเครื่องอ่านบัตรประจำตัวประชาชนแบบอเนกประสงค์ (2) กรณีไม่มีเครื่องอ่านบัตรประจำตัวประชาชนแบบอเนกประสงค์ IdP สามารถตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์จากผลการยืนยันตัวตนที่ส่งให้โดย IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 เป็นอย่างน้อย ทั้งนี้ การส่งผลการยืนยันตัวตนที่มีข้อมูลเกี่ยวกับอัตลักษณ์<u>ต้อง</u>ให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย (3) IdP <u>ต้อง</u>ตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ (4) IdP <u>ควร</u>ตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล

ระดับ IAL	ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์
	<u>กรณีใช้หนังสือเดินทางเป็นหลักฐานแสดงตน</u> (1) IdP <u>ต้อง</u>ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์จากเทคโนโลยีสื่อสารไร้สายระยะใกล้ (NFC) (2) IdP <u>ต้อง</u>ตรวจสอบสถานะของหนังสือเดินทางด้วยแหล่งข้อมูลที่น่าเชื่อถือ หรือตรวจสอบเอกสารสำคัญประจำตัวอื่นที่รัฐบาลไทยหรือหน่วยงานของรัฐเจ้าของสัญชาติออกให้ (เช่น ใบอนุญาตทำงาน ใบขับขี่) หรือตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ โดยใช้หมายเลขหลังบัตรประจำตัวประชาชน (laser code) (3) IdP <u>ควร</u>ตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล <u>กรณีใช้หลักฐานแสดงตนในรูปของข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือซึ่งออกโดยหน่วยงานของรัฐ</u> (1) IdP <u>ต้อง</u>ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตนในรูปของข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือด้วยระบบตรวจสอบของหน่วยงานของรัฐ (2) IdP <u>ควร</u>ตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล
IAL2.3	<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์เป็นหลักฐานแสดงตน</u> (1) IdP <u>ต้อง</u>ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์จากเครื่องอ่านบัตรประจำตัวประชาชนแบบอเนกประสงค์ (2) IdP <u>ต้อง</u>ตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ (3) IdP <u>ควร</u>ตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล <u>กรณีใช้หนังสือเดินทางเป็นหลักฐานแสดงตน</u> ข้อกำหนดเช่นเดียวกับ IAL2.2 <u>กรณีใช้หลักฐานแสดงตนในรูปของข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือซึ่งออกโดยหน่วยงานของรัฐ</u> ข้อกำหนดเช่นเดียวกับ IAL2.2
IAL3	<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์เป็นหลักฐานแสดงตน</u> (1) IdP <u>ต้อง</u>ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์จากเครื่องอ่านบัตรประจำตัวประชาชนแบบอเนกประสงค์ (2) IdP <u>ต้อง</u>ตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ (3) IdP <u>ต้อง</u>ตรวจสอบความมีอยู่จริงของอัตลักษณ์จากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติมอย่างน้อย 1 หน่วยงาน นอกเหนือจากฐานข้อมูลทะเบียนของกรมการปกครอง (เช่น ข้อมูลสิทธิประกันสุขภาพ จากสำนักงานหลักประกันสุขภาพแห่งชาติ)

ระดับ IAL	ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์
	(4) IdP ควรตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล กรณีใช้บัตรประจำตัวประชาชนในรูปของข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือเป็นหลักฐานแสดงตน (1) IdP ต้องตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์จากบัตรประจำตัวประชาชนในรูปของข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือด้วยระบบตรวจสอบของหน่วยงานของรัฐ (2) IdP ต้องตรวจสอบความมีอยู่จริงของอัตลักษณ์จากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติมอย่างน้อย 1 หน่วยงาน นอกเหนือจากฐานข้อมูลทะเบียนของกรมการปกครอง (เช่น ข้อมูลสิทธิประกันสุขภาพ จากสำนักงานหลักประกันสุขภาพแห่งชาติ) (3) IdP ควรตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล

4.3 ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์

ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์ตามระดับ IAL สามารถแสดงได้ตามตารางที่ 3

ตารางที่ 3 ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์

ระดับ IAL	ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์
IAL1	IdP ไม่จำเป็นต้องตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์
IAL2.1	(1) การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า**หรือ**แบบไม่พบเห็นต่อหน้า (2) IdP ต้องให้เจ้าหน้าที่เปรียบเทียบใบหน้าหรือภาพใบหน้าของบุคคล (visual comparison) กับภาพใบหน้าจากชิปของหลักฐานแสดงตน หรือภาพใบหน้าที่ส่งให้โดย IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 เป็นอย่างน้อย ทั้งนี้ การส่งภาพใบหน้าต้องให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย (3) กรณีพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า IdP ต้องบันทึกภาพใบหน้าของบุคคล เพื่อป้องกันการปฏิเสธว่าไม่ได้พิสูจน์ตัวตนหรือเพื่อใช้พิสูจน์ตัวตนอีกครั้ง
IAL2.2	(1) การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า**หรือ**แบบไม่พบเห็นต่อหน้า (2) IdP ต้องให้เจ้าหน้าที่เปรียบเทียบใบหน้าหรือภาพใบหน้าของบุคคล (visual comparison) กับภาพใบหน้าจากชิปหรือข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือของหลักฐานแสดงตน หรือภาพใบหน้าที่ส่งให้โดย IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 เป็นอย่างน้อย ทั้งนี้ การส่งภาพใบหน้าต้องให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย (3) กรณีพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า IdP ต้องบันทึกภาพใบหน้าของบุคคล เพื่อป้องกันการปฏิเสธว่าไม่ได้พิสูจน์ตัวตนหรือเพื่อใช้พิสูจน์ตัวตนอีกครั้ง
IAL2.3	(1) การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า**หรือ**แบบไม่พบเห็นต่อหน้า (2) IdP ต้องใช้วิธีการใดวิธีการหนึ่ง ดังนี้

ระดับ IAL	ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์
	(2.1) ใช้เทคโนโลยีเปรียบเทียบข้อมูลชีวมิติของบุคคล (biometric comparison) กับข้อมูลชีวมิติจากชิปหรือข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือของหลักฐานแสดงตน (2.2) เปรียบเทียบข้อมูลชีวมิติของบุคคลด้วยระบบตรวจสอบของหน่วยงานของรัฐ (3) กรณีพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า IdP ต้องบันทึกข้อมูลชีวมิติตั้งต้นของบุคคล (biometric sample) เพื่อป้องกันการปฏิเสธว่าไม่ได้พิสูจน์ตัวตนหรือเพื่อใช้พิสูจน์ตัวตนอีกครั้ง
IAL3	(1) การพิสูจน์ตัวตนแบบพบเห็นต่อหน้าเท่านั้น (2) IdP ต้องใช้วิธีการใดวิธีการหนึ่ง ดังนี้ (2.1) ใช้เทคโนโลยีเปรียบเทียบข้อมูลชีวมิติของบุคคล (biometric comparison) กับข้อมูลชีวมิติจากชิปหรือข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือของหลักฐานแสดงตน (2.2) เปรียบเทียบข้อมูลชีวมิติของบุคคลด้วยระบบตรวจสอบของหน่วยงานของรัฐ (3) IdP ต้องบันทึกข้อมูลชีวมิติตั้งต้นของบุคคล (biometric sample) เพื่อป้องกันการปฏิเสธว่าไม่ได้พิสูจน์ตัวตนหรือเพื่อใช้พิสูจน์ตัวตนอีกครั้ง

4.3.1 ข้อกำหนดของการเปรียบเทียบข้อมูลชีวมิติ

(1) การเปรียบเทียบข้อมูลชีวมิติต้องดำเนินการเปรียบเทียบแบบหนึ่งต่อหนึ่ง (one-to-one comparison) ระหว่างข้อมูลชีวมิติของบุคคลที่แสดงตนกับข้อมูลชีวมิติจากหลักฐานแสดงตนหรือจากหน่วยงานของรัฐ โดยไม่ทำการเปรียบเทียบแบบหนึ่งต่อกลุ่ม (one-to-many comparison) กับฐานข้อมูลที่มีข้อมูลชีวมิติของบุคคลมากกว่าหนึ่งคน

(2) ความแม่นยำในการเปรียบเทียบข้อมูลชีวมิติต้องมีอัตราการยอมรับที่ผิดพลาด (false accept rate: FAR)[2] ไม่เกิน 0.1% และอัตราการปฏิเสธที่ผิดพลาด (false reject rate: FRR)[3] ไม่เกิน 3%

(3) กรณีการพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า IdP ต้องมีเทคโนโลยีการตรวจจับการปลอมแปลงชีวมิติ (presentation attack detection) เช่น การตรวจจับการมีชีวิตของบุคคล (liveness detection) เพื่อช่วยป้องกันการโจมตีด้วยการใช้ภาพใบหน้าหรือลายนิ้วมือปลอม (spoofing attack) ทั้งนี้ IdP สามารถพิจารณาการทดสอบความสามารถของเทคโนโลยีการตรวจจับการปลอมแปลงชีวมิติให้สอดคล้องหรือเทียบเคียงได้ตามมาตรฐานสากล เช่น ISO/IEC 30107 Information technology – Biometric presentation attack detection หรือ FIDO Biometrics Requirements

4.4 สรุปข้อกำหนดที่สำคัญของการพิสูจน์ตัวตนตามระดับ IAL

ข้อกำหนดที่สำคัญของการพิสูจน์ตัวตนตามระดับ IAL แต่ละระดับสามารถสรุปได้ตามตารางที่ 4

[2] อัตราการยอมรับที่ผิดพลาด (FAR) คือ สัดส่วนของจำนวนครั้งที่ระบบยอมรับข้อมูลชีวมิติของบุคคลที่ไม่ถูกต้อง

[3] อัตราการปฏิเสธที่ผิดพลาด (FRR) คือ สัดส่วนของจำนวนครั้งที่ระบบปฏิเสธข้อมูลชีวมิติของบุคคลที่ถูกต้อง

ตารางที่ 4 สรุปข้อกำหนดที่สำคัญของการพิสูจน์ตัวตนตามระดับ IAL

ข้อกำหนดของการพิสูจน์ตัวตน	การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า					การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า				
	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3
การรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์										
รวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ ซึ่งเป็นข้อมูลที่บุคคลยืนยันด้วยตนเอง (self-asserted) เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจง	✓ (อาจ)					✓ (อาจ)				
รวบรวมข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตนอย่างน้อย 1 ฉบับ เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจง		✓ (ต้อง)	✓ (ต้อง)	✓ (ต้อง)			✓ (ต้อง)	✓ (ต้อง)	✓ (ต้อง)	
รวบรวมข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตนอย่างน้อย 1 ฉบับ และรวบรวมข้อมูลจากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติม เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจง										✓ (ต้อง)
การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์										
<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์</u> – ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์จากเครื่องอ่านบัตร – กรณีไม่มีเครื่องอ่านบัตร สามารถตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์จากผลการยืนยันตัวตนที่ส่งให้โดย IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 เป็นอย่างน้อย ทั้งนี้ การส่งผลการยืนยันตัวตนที่มีข้อมูลเกี่ยวกับอัตลักษณ์ต้องให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย		✓ (ต้อง)	✓ (ต้อง)				✓ (ต้อง)	✓ (ต้อง)		
<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์</u> – ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์จากเครื่องอ่านบัตร				✓ (ต้อง)					✓ (ต้อง)	✓ (ต้อง)
<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์</u> – ตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ			✓ (ต้อง)	✓ (ต้อง)				✓ (ต้อง)	✓ (ต้อง)	✓ (ต้อง)
<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์</u> – ตรวจสอบความมีอยู่จริงของอัตลักษณ์จากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติมอย่างน้อย 1 หน่วยงาน นอกเหนือจากฐานข้อมูลทะเบียนของกรมการปกครอง										✓ (ต้อง)

ข้อกำหนดของการพิสูจน์ตัวตน	การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า					การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า				
	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3
<u>กรณีใช้หนังสือเดินทาง</u> – ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์จากเทคโนโลยีสื่อสารไร้สายระยะใกล้ (NFC)		✓ (ต้อง)	✓ (ต้อง)	✓ (ต้อง)			✓ (ต้อง)	✓ (ต้อง)	✓ (ต้อง)	
<u>กรณีใช้หนังสือเดินทาง</u> – ตรวจสอบสถานะของหนังสือเดินทางด้วยแหล่งข้อมูลที่น่าเชื่อถือ หรือตรวจสอบเอกสารสำคัญประจำตัวอื่นที่รัฐบาลไทยหรือหน่วยงานของรัฐเจ้าของสัญชาติออกให้ หรือตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐโดยใช้หมายเลขหลังบัตรประจำตัวประชาชน (laser code)			✓ (ต้อง)	✓ (ต้อง)				✓ (ต้อง)	✓ (ต้อง)	
<u>กรณีใช้หลักฐานแสดงตนในรูปของข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือซึ่งออกโดยหน่วยงานของรัฐ</u> – ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตนในรูปของข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือด้วยระบบตรวจสอบของหน่วยงานของรัฐ			✓ (ต้อง)	✓ (ต้อง)				✓ (ต้อง)	✓ (ต้อง)	
<u>กรณีใช้บัตรประจำตัวประชาชนในรูปของข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือ</u> – ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์จากบัตรประจำตัวประชาชนในรูปของข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือด้วยระบบตรวจสอบของหน่วยงานของรัฐ – ตรวจสอบความมีอยู่จริงของอัตลักษณ์จากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติมอย่างน้อย 1 หน่วยงาน นอกเหนือจากฐานข้อมูลทะเบียนของกรมการปกครอง										✓ (ต้อง)
ตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล		✓ (ควร)	✓ (ควร)	✓ (ควร)			✓ (ควร)	✓ (ควร)	✓ (ควร)	✓ (ควร)
การตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์										
ให้เจ้าหน้าที่เปรียบเทียบใบหน้าหรือภาพใบหน้าของบุคคล (visual comparison) กับภาพใบหน้าจากชิปของหลักฐานแสดงตน หรือภาพใบหน้าที่ส่งให้โดย IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 เป็นอย่างน้อย ทั้งนี้ การส่งภาพใบหน้าต้องให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย		✓ (ต้อง)					✓ (ต้อง)			

ข้อกำหนดของการพิสูจน์ตัวตน	การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า					การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า				
	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3
ให้เจ้าหน้าที่เปรียบเทียบใบหน้าหรือภาพใบหน้าของบุคคล (visual comparison) กับภาพใบหน้าจากชิปหรือข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือของหลักฐานแสดงตน หรือภาพใบหน้าที่ส่งให้โดย IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 เป็นอย่างน้อย ทั้งนี้ การส่งภาพใบหน้าต้องให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย			✓ (ต้อง)					✓ (ต้อง)		
ใช้วิธีการใดวิธีการหนึ่ง ดังนี้ – ใช้เทคโนโลยีเปรียบเทียบข้อมูลชีวมิติของบุคคล (biometric comparison) กับข้อมูลชีวมิติจากชิปหรือข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือของหลักฐานแสดงตน – เปรียบเทียบข้อมูลชีวมิติของบุคคลด้วยระบบตรวจสอบของหน่วยงานของรัฐ				✓ (ต้อง)					✓ (ต้อง)	✓ (ต้อง)
มีเทคโนโลยีการตรวจจับการปลอมแปลงชีวมิติ (presentation attack detection) เช่น การตรวจจับการมีชีวิตของบุคคล (liveness detection) เพื่อช่วยป้องกันการโจมตีด้วยการใช้ภาพใบหน้าหรือลายนิ้วมือปลอม (spoofing attack)				✓ (ต้อง)						
บันทึกภาพใบหน้าหรือข้อมูลชีวมิติตั้งต้นของบุคคล (biometric sample) เพื่อป้องกันการปฏิเสธว่าไม่ได้พิสูจน์ตัวตนหรือเพื่อใช้พิสูจน์ตัวตนอีกครั้ง		✓ (ต้อง)	✓ (ต้อง)	✓ (ต้อง)			✓ (อาจ)	✓ (อาจ)	✓ (อาจ)	✓ (ต้อง)

บรรณานุกรม

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

[2] Digital Transformation Agency, Australian Government, "Trusted Digital Identity Framework (TDIF): 05 - Role Requirements", Release 4, September 2020, version 1.2.

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

[4] International Organization for Standardization, "ISO/IEC 30107-3:2017 Information technology – Biometric presentation attack detection – Part 3: Testing and reporting", September 2017.

[5] หนังสือกระทรวงมหาดไทย ที่ มท 0309.2/ว 6857 ลงวันที่ 22 มีนาคม 2556 เรื่อง การถ่ายสำเนาบัตรประจำตัวประชาชนแบบอเนกประสงค์ (Smart Card).