มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

ELECTRONIC TRANSACTION STANDARD

มธอ. 11 เล่ม 2-2569

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 2: ข้อกำหนดของการพิสูจน์ตัวตน

DIGITAL IDENTITY –
PART 2: IDENTITY PROOFING REQUIREMENTS

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.030

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 2: ข้อกำหนดของการพิสูจน์ตัวตน

มธอ. 11 เล่ม 2-2569

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ศูนย์ราชการเฉลิมพระเกียรติฯ (อาคารซี) ชั้นที่ 4 เลขที่ 120 หมู่ที่ 3 ซอยแจ้งวัฒนะ 7
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ประธานกรรมการ

นางวิลาวรรณ มังคละธนะกุล

รองประธานกรรมการ

นายพชร อนันตศิลป์ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

กรรมการผู้ทรงคุณวุฒิ

นายกอบศักดิ์ ดวงดี
นายทวีลาภ ฤทธาภิรมย์
นางปิยนุช วุฒิสอน
นายศักรินทร์ ร่วมรังษี
นายเฉลิมรัฐ นาควิเชียร
นายสุพันธุ์ ตั้งจิตกุศลมั่น
นางสาวอ้อนฟ้า เวชชาชีวะ

กรรมการและเลขานุการ

นายชัยชนะ มิตรพันธ์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คณะอนุกรรมการกลั่นกรองการกำหนดหลักเกณฑ์ในการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ประธานอนุกรรมการ

นางสาวอัจฉรินทร์ พัฒนพันธ์ชัย

อนุกรรมการ

นายอารยะ ไข่มุกด์	สำนักงานปลัดกระทรวงสาธารณสุข
นางสาวสุชาดา คำวงษ์	กรมการปกครอง
นายพลากรณ์ พูลเพิ่ม	กรมการกงสุล
นางศิริพร ชำนาญชาติ	กรมพัฒนาธุรกิจการค้า
นายพรรคธาดา ตรีรัตนพิทักษ์	ธนาคารแห่งประเทศไทย
นางสาวสายชล แซ่ลี้	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
นางสาวอรวรี เจริญพร	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
นายสมเกียรติ วัฒนาประสบสุข	สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
นายเฉลิมศักย์ ดาสะอาด	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
นายวิบูลย์ ภัทรพิบูล	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
นายสรรเพชร แสงเนตรสว่าง	สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายปรนนท์ ฐิตะวรรโณ	คณะกรรมการร่วมภาคเอกชน ๓ สถาบัน
นายวิเชียร เปรมชัยสวัสดิ์	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นายเฉลิมรัฐ นาควิเชียร	

เลขานุการ

นางสาวพิชญลักษณ์ เอกะพยัคฆ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คำนำ

ด้วยการเข้าทำธุรกรรมต่าง ๆ จำเป็นต้องมีกระบวนการพิสูจน์และยืนยันตัวตนผู้ที่ประสงค์จะเข้าทำธุรกรรมก่อนเพื่อให้มั่นใจได้ว่าผู้ที่ประสงค์จะเข้าทำธุรกรรมเป็นบุคคลนั้นจริง ประกอบกับในปัจจุบันมีการทำธุรกรรมและการให้บริการในรูปแบบดิจิทัลเพิ่มมากขึ้น ผู้ให้บริการจึงเริ่มมีการพัฒนากระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัลเพื่ออำนวยความสะดวกในการเข้าใช้บริการต่าง ๆ ในขณะเดียวกันกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ได้มีการแก้ไขปรับปรุงเพื่อรองรับให้บุคคลสามารถพิสูจน์และยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ ซึ่งกลไกดังกล่าวสามารถลดภาระต่อผู้ใช้บริการในการแสดงตน การส่งเอกสารหรือหลักฐานประกอบการพิสูจน์และยืนยันตัวตน รวมถึงช่วยลดขั้นตอนที่ต้องทำกระบวนการเดิมซ้ำ ๆ เพื่อพิสูจน์ตัวตนก่อนเข้าทำธุรกรรม

อย่างไรก็ตาม กระบวนการพิสูจน์และยืนยันตัวตนในปัจจุบันยังมีความหลากหลายและมีข้อกำหนดแตกต่างกันไปตามเงื่อนไขและความจำเป็นของผู้ให้บริการหรือหน่วยงานแต่ละแห่งซึ่งในบางกรณีอาจเกิดความไม่สอดคล้องหรือไม่สามารถนำมาใช้งานร่วมกันได้ ดังนั้น จึงได้มีการพัฒนามาตรฐานเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยการดำเนินการที่ผ่านมาสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชนได้ร่วมกันจัดทำมาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัล ได้แก่ ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ (ETDA Recommendation) ซึ่งมีการพัฒนาและปรับปรุงมาอย่างต่อเนื่อง ดังนี้

- เวอร์ชัน 1.0: เลขที่ ขมธอ. 18-2561, 19-2561 และ 20-2561
- เวอร์ชัน 2.0: เลขที่ ขมธอ. 18-2564, 19-2564 และ 20-2564
- เวอร์ชัน 3.0: เลขที่ ขมธอ. 18-2566, 19-2566 และ 20-2566

ในการนี้ เพื่อให้เกิดความสอดคล้องและเสริมสร้างความน่าเชื่อถือและยอมรับในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล และเพื่อให้ผู้ให้บริการและหน่วยงานต่าง ๆ สามารถใช้อ้างอิงและเลือกใช้งานดิจิทัลไอดีร่วมกันได้บนมาตรฐานและระดับความน่าเชื่อถือที่มีความสอดคล้องกัน คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงเห็นควรให้มีการยกระดับมาตรฐานดังกล่าว โดยนำข้อเสนอแนะมาตรฐานฯ เลขที่ ขมธอ. 18-2566, 19-2566 และ 20-2566 มาปรับปรุงเป็นชุดมาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล (เลขที่ มธอ. 11) ซึ่งประกอบด้วย

- เล่ม 1 กรอบการทำงาน (Part 1: Framework)
- เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน (Part 2: Identity Proofing Requirements)
- เล่ม 3 ข้อกำหนดของการยืนยันตัวตน (Part 3: Authentication Requirements)

สำหรับการพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน ฉบับนี้ เป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการพิสูจน์ตัวตนของบุคคลที่ประสงค์จะใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้ IdP มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกันตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ เลขที่ มธอ. 11 เล่ม 2-2566 ได้ถูกยกเลิกและแทนที่ด้วยมาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ เลขที่ มธอ. 11 เล่ม 2-2569 ฉบับนี้ ซึ่งพัฒนาต่อยอดจากฉบับเดิม โดยมีการปรับปรุงเนื้อหาทางเทคนิคให้มีความชัดเจนยิ่งขึ้น เพิ่มความสะดวกในการใช้งาน และสอดคล้องกับแนวปฏิบัติในปัจจุบัน

สารบัญ

หน้า

1. ขอบข่าย **1**

2. การพิสูจน์ตัวตน **1**

2.1 การรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ 1

2.2 การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ 2

2.3 การตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์ 2

3. ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL) **2**

3.1 ระดับ IAL1 2

3.2 ระดับ IAL2 2

3.3 ระดับ IAL3 3

4. ข้อกำหนดของการพิสูจน์ตัวตน **3**

4.1 ข้อกำหนดของการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ 3

4.2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ 4

4.3 ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์ 6

4.3.1 ข้อกำหนดของการเปรียบเทียบข้อมูลชีวมิติ 7

4.3.2 ข้อกำหนดของการเปรียบเทียบข้อมูลชีวมิติ กรณีใช้บริการระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (face verification service: FVS) ของกรมการปกครอง 7

4.4 สรุปข้อกำหนดที่สำคัญของการพิสูจน์ตัวตนตามระดับ IAL 8

ภาคผนวก ก. อินโฟกราฟิกส์ของระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) **12**

บรรณานุกรม **13**

สารบัญตาราง

หน้า

ตารางที่ 1 ข้อกำหนดของการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ 3

ตารางที่ 2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ 4

ตารางที่ 3 ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์ 6

ตารางที่ 4 สรุปข้อกำหนดที่สำคัญของการพิสูจน์ตัวตนตามระดับ IAL 9

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 2: ข้อกำหนดของการพิสูจน์ตัวตน

1. ขอบข่าย

มาตรฐานฉบับนี้เป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการพิสูจน์ตัวตนของบุคคลที่ประสงค์จะใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้ IdP มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกันตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)

มาตรฐานฉบับนี้เป็นข้อกำหนดสำหรับหน่วยงานที่ให้บริการพิสูจน์และยืนยันตัวตนแก่บุคคลภายนอก ข้อกำหนดในมาตรฐานฉบับนี้สามารถประยุกต์ใช้ได้กับบริการพิสูจน์และยืนยันตัวตนที่ใช้เพื่อประโยชน์ภายในกิจการของตนเอง ทั้งนี้ ไม่มีเจตนาปิดกั้นหรือห้ามใช้วิธีการอื่นเพื่อเพิ่มประสิทธิภาพของการพิสูจน์และยืนยันตัวตน

มาตรฐานฉบับนี้มีรูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) ดังต่อไปนี้

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

2. การพิสูจน์ตัวตน

การพิสูจน์ตัวตน (identity proofing) เป็นกระบวนการที่ IdP รวบรวมและตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคล และตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์นั้น โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าอัตลักษณ์ที่กล่าวอ้างเป็นอัตลักษณ์ของบุคคลนั้นจริงตามระดับความน่าเชื่อถือที่กำหนด โดยผลลัพธ์ที่คาดหวังจากการพิสูจน์ตัวตนของบุคคลที่ประสงค์จะมีดิจิทัลไอดีสำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ประกอบด้วย

- สามารถแยกแยะอัตลักษณ์ที่กล่าวอ้างว่าอัตลักษณ์นั้นมีเพียงอันเดียวและมีความเฉพาะเจาะจงในบริบทของบริการธุรกรรม
- สามารถตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ว่ามีความถูกต้อง แท้จริง และเป็นปัจจุบัน
- สามารถตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับข้อมูลเกี่ยวกับอัตลักษณ์ที่กล่าวอ้าง

การพิสูจน์ตัวตนประกอบด้วยกระบวนการพื้นฐาน 3 กระบวนการ ดังนี้ [1]

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 ตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับข้อมูลเกี่ยวกับอัตลักษณ์ที่กล่าวอ้าง เพื่อพิสูจน์ว่าบุคคลที่กำลังพิสูจน์ตัวตนเป็นเจ้าของข้อมูลเกี่ยวกับอัตลักษณ์ดังกล่าวจริง

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 อาจมีการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์หรือการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์ด้วยวิธีการอื่น ๆ ตามความเสี่ยงของบริการธุรกรรม นอกเหนือจากวิธีการที่กำหนดไว้ในระดับ IAL2 และ IAL3 เช่น

- ตรวจสอบสำเนาหรือรูปถ่ายของหลักฐานแสดงตน [1]
- ตรวจสอบลักษณะทางกายภาพของหลักฐานแสดงตนโดยเจ้าหน้าที่
- ตรวจสอบข้อมูลของหลักฐานแสดงตนและตรวจสอบสถานะของหลักฐานแสดงตน
- เปรียบเทียบใบหน้าหรือภาพใบหน้าของบุคคลกับภาพใบหน้าของหลักฐานแสดงตน
- ยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ (เช่น หมายเลขโทรศัพท์ อีเมล)

3.2 ระดับ IAL2

ระดับ IAL2 กำหนดให้มีการขอหลักฐานแสดงตน การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ว่าอัตลักษณ์ที่กล่าวอ้างเป็นข้อมูลของบุคคลที่มีอยู่จริง และการตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตน

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

กับข้อมูลเกี่ยวกับอัตลักษณ์นั้น ทั้งนี้ การพิสูจน์ตัวตนที่ระดับ IAL2 สามารถทำได้ทั้งแบบพบเห็นต่อหน้า (face-to-face) หรือแบบไม่พบเห็นต่อหน้า (non face-to-face) เช่น การพิสูจน์ตัวตนผ่านเครื่องให้บริการ (kiosk) หรือแอปพลิเคชันของ IdP

IdP ที่รองรับระดับ IAL2 สามารถส่งผลการยืนยันตัวตนที่มีข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลนั้นให้กับ RP ที่ต้องการระดับ IAL เท่ากันหรือต่ำกว่าได้ หากได้รับความยินยอมจากบุคคลที่เป็นเจ้าของข้อมูล

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

3.3 ระดับ IAL3

ระดับ IAL3 เพิ่มความเข้มงวดจากระดับ IAL2 โดยกำหนดให้มีการตรวจสอบความมีอยู่จริงของอัตลักษณ์จากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติม และการตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับข้อมูลเกี่ยวกับอัตลักษณ์ด้วยการเปรียบเทียบข้อมูลชีวมิติ (biometric comparison) เพื่อป้องกันการปลอมตัวเป็นบุคคลอื่นและการลงทะเบียนซ้ำ ทั้งนี้ การพิสูจน์ตัวตนที่ระดับ IAL3 ต้องทำแบบพบเห็นต่อหน้า (face-to-face) เท่านั้น

IdP ที่รองรับระดับ IAL3 สามารถส่งผลการยืนยันตัวตนที่มีข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลนั้นให้กับ 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 และจากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติม (นอกเหนือจากฐานข้อมูลทะเบียนของกรมการปกครอง) เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจง (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) กรณีมีเครื่องอ่านบัตรประจำตัวประชาชน IdP <u>ต้อง</u>ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตรประจำตัวประชาชน เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของบัตรประจำตัวประชาชน (2) กรณีไม่มีเครื่องอ่านบัตรประจำตัวประชาชน IdP <u>ต้อง</u>ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ โดยใช้ข้อมูลจากผลการยืนยันตัวตนผ่าน IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 ขึ้นไป ทั้งนี้ การส่งผลการยืนยันตัวตนที่มีข้อมูลเกี่ยวกับอัตลักษณ์ต้องให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย (3) IdP <u>ควร</u>ตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล <u>กรณีใช้หนังสือเดินทางเป็นหลักฐานแสดงตน</u> (1) IdP <u>ต้อง</u>ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เทคโนโลยีสื่อสารไร้สายระยะใกล้ (near field communication: NFC) เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของหนังสือเดินทาง (2) IdP <u>ควร</u>ตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล
IAL2.2	<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์เป็นหลักฐานแสดงตน</u> (1) กรณีมีเครื่องอ่านบัตรประจำตัวประชาชน IdP <u>ต้อง</u>ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตรประจำตัวประชาชน เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของบัตรประจำตัวประชาชน (2) กรณีไม่มีเครื่องอ่านบัตรประจำตัวประชาชน IdP <u>ต้อง</u>ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ โดยใช้ข้อมูลจากผลการยืนยันตัวตนผ่าน IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 ขึ้นไป ทั้งนี้ การส่งผลการยืนยันตัวตนที่มีข้อมูลเกี่ยวกับอัตลักษณ์ต้องให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย (3) IdP <u>ต้อง</u>ตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ โดยใช้หมายเลขชิป (chip number) กรณีมีเครื่องอ่านบัตรประจำตัวประชาชน หรือใช้หมายเลขหลังบัตรประจำตัวประชาชน (laser code) กรณีไม่มีเครื่องอ่านบัตรประจำตัวประชาชน

ระดับ IAL	ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์
	(4) IdP ควรตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล กรณีใช้หนังสือเดินทางเป็นหลักฐานแสดงตน (1) IdP ต้องตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เทคโนโลยีสื่อสารไร้สายระยะใกล้ (NFC) เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของหนังสือเดินทาง (2) IdP ต้องตรวจสอบสถานะของหนังสือเดินทางด้วยแหล่งข้อมูลที่น่าเชื่อถือ หรือตรวจสอบเอกสารสำคัญประจำตัวอื่นที่รัฐบาลไทยหรือหน่วยงานของรัฐเจ้าของสัญชาติออกให้ (เช่น ใบอนุญาตทำงาน ใบขับขี่) หรือตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ โดยใช้หมายเลขหลังบัตรประจำตัวประชาชน (laser code) (3) IdP ควรตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล
IAL2.3	กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์เป็นหลักฐานแสดงตน (1) กรณีมีเครื่องอ่านบัตรประจำตัวประชาชน IdP ต้องตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตรประจำตัวประชาชน เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของบัตรประจำตัวประชาชน และตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ โดยใช้หมายเลขชิป (chip number) (2) กรณีไม่มีเครื่องอ่านบัตรประจำตัวประชาชน IdP ต้องได้รับอนุญาตให้ใช้บริการระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (face verification service) ของกรมการปกครอง [2] โดย IdP ต้องตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ด้วยการยืนยันตัวตนเจ้าของข้อมูลตามหลักเกณฑ์หรือวิธีการที่กรมการปกครองกำหนด (3) IdP ควรตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล กรณีใช้หนังสือเดินทางเป็นหลักฐานแสดงตน ข้อกำหนดเช่นเดียวกับ IAL2.2

[2] ระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (face verification service: FVS) คือ ระบบที่กรมการปกครองได้จัดสร้างและพัฒนาขึ้น เพื่อให้บริการเปรียบเทียบ (matching) ข้อมูลชีวมิติจากภาพใบหน้าของบุคคล กับข้อมูลภาพใบหน้าของบุคคลดังกล่าวในฐานข้อมูลทะเบียนประวัติราษฎรของสำนักทะเบียนกลางแบบหนึ่งต่อหนึ่ง (one-to-one) โดยการแจ้งผลการเปรียบเทียบแก่ผู้ใช้บริการในรูปแบบคะแนนความเหมือนเป็นร้อยละ (match score) เพื่อวัตถุประสงค์ในการพิสูจน์ตัวตนของบุคคล [6]

ระดับ IAL	ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์
IAL3	กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์เป็นหลักฐานแสดงตน (1) IdP ต้องตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตรประจำตัวประชาชน เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของบัตรประจำตัวประชาชน และตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ โดยใช้หมายเลขชิป (chip number) (2) IdP ต้องตรวจสอบความมีอยู่จริงของอัตลักษณ์จากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติมอย่างน้อย 1 หน่วยงาน นอกเหนือจากฐานข้อมูลทะเบียนของกรมการปกครอง (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) กับภาพใบหน้าจากชิปของหลักฐานแสดงตนของหน่วยงานของรัฐ หรือภาพใบหน้าจาก IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 ขึ้นไป ทั้งนี้ การส่งภาพใบหน้าต้องให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย (3) กรณีพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า IdP ต้องบันทึกภาพใบหน้าของบุคคล เพื่อป้องกันการปฏิเสธว่าไม่ได้พิสูจน์ตัวตนหรือเพื่อใช้พิสูจน์ตัวตนอีกครั้ง
IAL2.2	ข้อกำหนดเช่นเดียวกับ IAL2.1
IAL2.3	(1) การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า**หรือ**แบบไม่พบเห็นต่อหน้า (2) IdP ต้องเปรียบเทียบข้อมูลชีวมิติ (biometric comparison) โดยใช้วิธีการใดวิธีการหนึ่ง ดังนี้ (2.1) IdP ใช้เทคโนโลยีชีวมิติในการเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของบุคคลกับข้อมูลชีวมิติจากชิปของหลักฐานแสดงตนของหน่วยงานของรัฐ (2.2) IdP ใช้ระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (face verification service) ของกรมการปกครองในการเปรียบเทียบภาพใบหน้าของบุคคลกับฐานข้อมูลชีวมิติ (3) กรณีพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า IdP ต้องบันทึกข้อมูลชีวมิติตั้งต้นของบุคคล (biometric sample) เพื่อป้องกันการปฏิเสธว่าไม่ได้พิสูจน์ตัวตนหรือเพื่อใช้พิสูจน์ตัวตนอีกครั้ง

ระดับ IAL	ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์
IAL3	(1) การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า**เท่านั้น** (2) IdP ต้องเปรียบเทียบข้อมูลชีวมิติ (biometric comparison) โดยใช้วิธีการใดวิธีการหนึ่ง ดังนี้ (2.1) IdP ใช้เทคโนโลยีชีวมิติในการเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของบุคคลกับข้อมูลชีวมิติจากชิปของหลักฐานแสดงตนของหน่วยงานของรัฐ (2.2) IdP ใช้ระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (face verification service) ของกรมการปกครองในการเปรียบเทียบภาพใบหน้าของบุคคลกับฐานข้อมูลชีวมิติ (3) IdP ต้องบันทึกข้อมูลชีวมิติตั้งต้นของบุคคล (biometric sample) เพื่อป้องกันการปฏิเสธว่าไม่ได้พิสูจน์ตัวตนหรือเพื่อใช้พิสูจน์ตัวตนอีกครั้ง

4.3.1 ข้อกำหนดของการเปรียบเทียบข้อมูลชีวมิติ

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

(2) ความแม่นยำในการเปรียบเทียบข้อมูลชีวมิติต้องมีอัตราการเข้าคู่ผิดพลาด (false match rate: FMR) ไม่เกิน 0.01% และอัตราการไม่เข้าคู่ผิดพลาด (false non-match rate: FNMR) ไม่เกิน 3% [2]

(3) กรณีการพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า IdP ต้องมีเทคโนโลยีการตรวจจับการโจมตีหลอกระบบ (presentation attack detection: PAD) เช่น การตรวจจับการมีชีวิต (liveness detection) เพื่อช่วยป้องกันการโจมตีด้วยการใช้ภาพใบหน้าหรือลายนิ้วมือปลอม (spoofing attack) ทั้งนี้ IdP สามารถพิจารณาการทดสอบความสามารถของเทคโนโลยีการตรวจจับการโจมตีหลอกระบบ (PAD) ให้สอดคล้องหรือเทียบเคียงได้ตามมาตรฐานสากล เช่น ISO/IEC 30107 Information technology – Biometric presentation attack detection หรือ FIDO Biometrics Requirements

4.3.2 ข้อกำหนดของการเปรียบเทียบข้อมูลชีวมิติ กรณีใช้บริการระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (face verification service: FVS) ของกรมการปกครอง

(1) IdP ต้องควบคุมการจัดเก็บ (capture) ภาพใบหน้าของบุคคล เพื่อใช้ในการเปรียบเทียบข้อมูลชีวมิติจากภาพใบหน้า ให้ดำเนินการโดยระบบของ IdP โดยตรงเท่านั้น

(2) IdP ต้องมีเทคโนโลยีการตรวจจับการโจมตีหลอกระบบ (presentation attack detection: PAD) เช่น การตรวจจับการมีชีวิต (liveness detection) เพื่อช่วยป้องกันการโจมตีด้วยการใช้ภาพใบหน้าหรือลายนิ้วมือปลอม (spoofing attack) ทั้งนี้ IdP สามารถพิจารณาการทดสอบความสามารถของเทคโนโลยีการตรวจจับการโจมตีหลอกระบบ (PAD) ให้สอดคล้องหรือเทียบเคียงได้ตามมาตรฐานสากล เช่น ISO/IEC 30107 Information technology – Biometric presentation attack detection หรือ FIDO Biometrics Requirements

(3) IdP ต้องควบคุมให้ภาพใบหน้าของบุคคลที่ได้จากการจัดเก็บจากระบบของหน่วยงาน มีคุณภาพดีตามที่กรมการปกครองกำหนด เพื่อให้การเปรียบเทียบข้อมูลชีวมิติจากภาพใบหน้าด้วยระบบ FVS มีประสิทธิภาพและมีความแม่นยำ ทั้งนี้ การควบคุมคุณภาพของภาพใบหน้า อย่างน้อยต้องคำนึงถึงชนิดของภาพ (ภาพสีหรือภาพระดับเทา) ขนาดภาพ ความละเอียดของภาพ และขนาดใบหน้าที่ปรากฏบนภาพ

(4) IdP ต้องจัดทำคำขอเปรียบเทียบภาพใบหน้า พร้อมด้วยข้อมูลเลขประจำตัวประชาชน และภาพใบหน้าของบุคคลที่จัดเก็บ เพื่อใช้ในการเปรียบเทียบภาพใบหน้ากับระบบ FVS

(5) IdP ต้องจัดทำรายละเอียดของกระบวนการควบคุมคุณภาพของภาพใบหน้า พร้อมหลักเกณฑ์และผลการพิจารณาของ IdP ในการพิจารณาผลเปรียบเทียบจากค่าคะแนนความเหมือนที่ได้รับแจ้งจากระบบ FVS เพื่อพิสูจน์ตัวตนของบุคคล

4.4 สรุปข้อกำหนดที่สำคัญของการพิสูจน์ตัวตนตามระดับ IAL

ข้อกำหนดที่สำคัญของการพิสูจน์ตัวตนตามระดับ IAL แต่ละระดับสามารถสรุปได้ตามตารางที่ 4

ตารางที่ 4 สรุปข้อกำหนดที่สำคัญของการพิสูจน์ตัวตนตามระดับ IAL

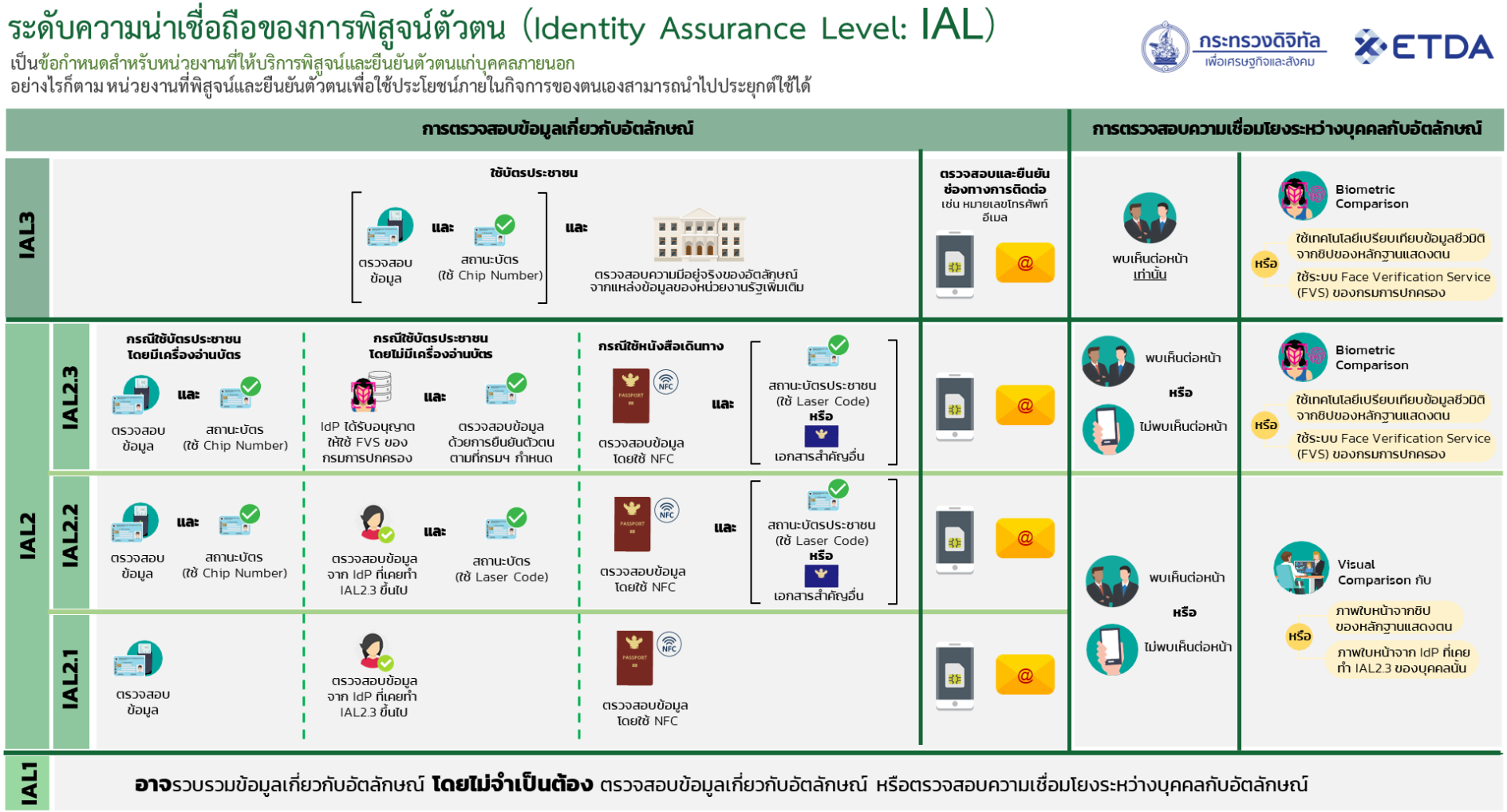
ข้อกำหนดของการพิสูจน์ตัวตน	การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า					การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า				
	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3
การรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์										
รวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ ซึ่งเป็นข้อมูลที่บุคคลยืนยันด้วยตนเอง (self-asserted) เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจง	✓ (อาจ)					✓ (อาจ)				
รวบรวมข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตนอย่างน้อย 1 ฉบับ เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจง		✓ (ต้อง)	✓ (ต้อง)	✓ (ต้อง)			✓ (ต้อง)	✓ (ต้อง)	✓ (ต้อง)	
รวบรวมข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตนอย่างน้อย 1 ฉบับ และจากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติม (นอกเหนือจากฐานข้อมูลทะเบียนของกรมการปกครอง) เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจง										✓ (ต้อง)
การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์										
<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์</u> – <u>กรณีมีเครื่องอ่านบัตร</u> ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตร เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของบัตรประจำตัวประชาชน – <u>กรณีไม่มีเครื่องอ่านบัตร</u> ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ โดยใช้ข้อมูลจากผลการยืนยันตัวตนผ่าน IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 ขึ้นไป ทั้งนี้ การส่งผลการยืนยันตัวตนที่มีข้อมูลเกี่ยวกับอัตลักษณ์ต้องให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย		✓ (ต้อง)	✓ (ต้อง)				✓ (ต้อง)	✓ (ต้อง)		
<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์</u> – ตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ โดยใช้หมายเลขชิป (chip number) กรณีมีเครื่องอ่านบัตร หรือใช้หมายเลขหลังบัตรประจำตัวประชาชน (laser code) กรณีไม่มีเครื่องอ่านบัตร			✓ (ต้อง)					✓ (ต้อง)		

ข้อกำหนดของการพิสูจน์ตัวตน	การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า					การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า				
	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3
<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์</u> – <u>กรณีมีเครื่องอ่านบัตร</u> ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตร เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของบัตรประจำตัวประชาชน และตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานรัฐ โดยใช้หมายเลขชิป (chip number) – <u>กรณีไม่มีเครื่องอ่านบัตร</u> IdP ต้องได้รับอนุญาตให้ใช้บริการระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (face verification service) ของกรมการปกครอง โดยตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ด้วยการยืนยันตัวตนเจ้าของข้อมูลตามหลักเกณฑ์หรือวิธีการที่กรมการปกครองกำหนด				✓ (ต้อง)					✓ (ต้อง)	
<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์</u> – ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตร เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของบัตรประจำตัวประชาชน และตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานรัฐ โดยใช้หมายเลขชิป (chip number) – ตรวจสอบความมีอยู่จริงของอัตลักษณ์จากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติมอย่างน้อย 1 หน่วยงาน นอกเหนือจากฐานข้อมูลทะเบียนของกรมการปกครอง										✓ (ต้อง)
<u>กรณีใช้หนังสือเดินทาง</u> – ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เทคโนโลยีสื่อสารไร้สายระยะใกล้ (NFC) เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของหนังสือเดินทาง		✓ (ต้อง)	✓ (ต้อง)	✓ (ต้อง)			✓ (ต้อง)	✓ (ต้อง)	✓ (ต้อง)	
<u>กรณีใช้หนังสือเดินทาง</u> – ตรวจสอบสถานะของหนังสือเดินทางด้วยแหล่งข้อมูลที่น่าเชื่อถือ หรือตรวจสอบเอกสารสำคัญประจำตัวอื่นที่รัฐบาลไทยหรือหน่วยงานของรัฐเจ้าของสัญชาติออกให้ หรือตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ โดยใช้หมายเลขหลังบัตรประจำตัวประชาชน (laser code)			✓ (ต้อง)	✓ (ต้อง)				✓ (ต้อง)	✓ (ต้อง)	

ข้อกำหนดของการพิสูจน์ตัวตน	การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า					การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า				
	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3
ตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล		✓ (ควร)	✓ (ควร)	✓ (ควร)			✓ (ควร)	✓ (ควร)	✓ (ควร)	✓ (ควร)
การตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์										
ให้เจ้าหน้าที่เปรียบเทียบใบหน้าหรือภาพใบหน้าของบุคคล (visual comparison) กับภาพใบหน้าจากชิปของหลักฐานแสดงตนของหน่วยงานของรัฐ หรือภาพใบหน้าจาก IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 ขึ้นไป ทั้งนี้ การส่งภาพใบหน้าต้องให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย		✓ (ต้อง)	✓ (ต้อง)				✓ (ต้อง)	✓ (ต้อง)		
เปรียบเทียบข้อมูลชีวมิติ (biometric comparison) โดยใช้วิธีการใดวิธีการหนึ่ง ดังนี้ – IdP ใช้เทคโนโลยีชีวมิติในการเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของบุคคลกับข้อมูลชีวมิติจากชิปของหลักฐานแสดงตนของหน่วยงานของรัฐ – IdP ใช้ระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (face verification service) ของกรมการปกครองในการเปรียบเทียบภาพใบหน้าของบุคคลกับฐานข้อมูลชีวมิติ				✓ (ต้อง)					✓ (ต้อง)	✓ (ต้อง)
มีเทคโนโลยีการตรวจจับการโจมตีหลอกระบบ (presentation attack detection: PAD) เช่น การตรวจจับการมีชีวิต (liveness detection) เพื่อช่วยป้องกันการโจมตีด้วยการใช้ภาพใบหน้าหรือลายนิ้วมือปลอม (spoofing attack)				✓ (ต้อง)						
บันทึกภาพใบหน้าหรือข้อมูลชีวมิติตั้งต้นของบุคคล (biometric sample) เพื่อป้องกันการปฏิเสธว่าไม่ได้พิสูจน์ตัวตนหรือเพื่อใช้พิสูจน์ตัวตนอีกครั้ง		✓ (ต้อง)	✓ (ต้อง)	✓ (ต้อง)						✓ (ต้อง)

ภาคผนวก ก. อินโฟกราฟิกส์ของระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL)

อินโฟกราฟิกส์ (infographics) ของระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL) ซึ่งเป็นการสรุปข้อกำหนดที่สำคัญบางส่วนจากมาตรฐานเพื่อนำเสนอข้อมูลเป็นภาพที่สามารถเข้าใจได้ง่าย แสดงตามนี้



หมายเหตุ: เป็นการสรุปข้อกำหนดที่สำคัญบางส่วนจากมาตรฐาน

ศึกษารายละเอียดจาก มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน (เลขที่ มธอ. 11 เล่ม 2-2569)

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 4.7, June 2022.

[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).

[6] ประกาศกรมการปกครอง เรื่อง หลักเกณฑ์การอนุญาตให้หน่วยงานของรัฐและหน่วยงานเอกชนใช้บริการระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (DOPA-Digital ID) และระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (Face Verification Service : FVS) ของกรมการปกครอง, 18 มิถุนายน 2567.