ETDA สพธอ
www.etda.or.th

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard for Electronic Transactions

ขมธอ. 19-2561

ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน

DIGITAL IDENTITY GUIDELINE FOR THAILAND – ENROLMENT AND IDENTITY PROOFING

เวอร์ชัน 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ICS 35.030

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน

ขมธอ. 19-2561

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

ประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ 28 กันยายน พ.ศ. 2561

คณะทำงานนำร่องการใช้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ประธานคณะทำงานร่วม

นางสาวสิริธิดา พนมวัน ณ อยุธยา	ธนาคารแห่งประเทศไทย
นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

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 (องค์การมหาชน)
นายธนฉัตร วิจารณ์ปรีชา	ธนาคารเกียรตินาคิน จำกัด (มหาชน)

ผู้ช่วยเลขานุการ

นายนครินทร์ ลิ้มรังษี	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน ฉบับนี้ จัดทำขึ้นเพื่อเป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการลงทะเบียน (enrolment) และพิสูจน์ตัวตน (identity proofing) ของผู้สมัครใช้บริการที่ประสงค์จะทำธุรกรรมออนไลน์ด้วยดิจิทัลไอดี (digital identity) เพื่อให้ IdP มีแนวทางในการลงทะเบียนและพิสูจน์ตัวตนของผู้สมัครใช้บริการตามระดับความน่าเชื่อถือของไอเดนทิตี (identity assurance level: IAL) ที่เป็นมาตรฐานเดียวกัน โดยพัฒนาตามแนวมาตรฐานของ NIST Special Publication 800-63A – Digital Identity Guidelines – Enrollment and Identity Proofing, National Institute of Standards and Technology, US Department of Commerce, June 2017

และได้มีการรับฟังความคิดเห็นจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความครบถ้วนสมบูรณ์ และสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน ฉบับนี้ จัดทำขึ้นตามความร่วมมือด้านการมาตรฐานระหว่างหน่วยงานภาครัฐและเอกชนในคณะทำงานนำร่องการใช้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ร่วมกับ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200
E-mail: estandard.center@etda.or.th
Website: www.etda.or.th

คำนำ

การให้บริการของรัฐแก่ประชาชนและภาคธุรกิจหรือการให้บริการของภาคธุรกิจแก่ประชาชนในปัจจุบัน ประกอบด้วยขั้นตอนการพิสูจน์และยืนยันตัวตนที่มีความซับซ้อน มีความสิ้นเปลืองทั้งเวลาและทรัพยากร เกิดภาระแก่ทั้งผู้แสดงตนและผู้มีหน้าที่ในการตรวจสอบความถูกต้องและยืนยันตัวตน รัฐบาลจึงได้ดำเนินงานพัฒนาระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID Platform) ที่สอดคล้องกับนโยบายอำนวยความสะดวกในการประกอบธุรกิจ (Ease of Doing Business) และการให้บริการกับประชาชน เพื่อให้เป็นโครงสร้างพื้นฐานทางดิจิทัลที่สำคัญของประเทศ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน ได้ร่วมกันกำหนดแนวทางการพัฒนาระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของประเทศ และจัดทำมาตรฐานเกี่ยวกับแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย (Digital Identity Guideline for Thailand) ขึ้น ประกอบด้วยมาตรฐานทั้งหมด 3 ฉบับ ดังนี้

(1) แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ (Overview and Glossary)

เป็นเอกสารอธิบายภาพรวมและอภิธานศัพท์เกี่ยวกับการใช้งานดิจิทัลไอดีสำหรับประเทศไทย การบริหารความเสี่ยง และการกำหนดระดับความน่าเชื่อถือ

(2) แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน (Enrolment and Identity Proofing)

เป็นเอกสารอธิบายข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการลงทะเบียนและพิสูจน์ตัวตนของผู้สมัครใช้บริการที่ประสงค์จะทำธุรกรรมออนไลน์ด้วยดิจิทัลไอดี (digital identity) ตามระดับความน่าเชื่อถือของไอเดนทิตี (identity assurance level: IAL)

(3) แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน (Authentication)

เป็นเอกสารอธิบายข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการกำหนดและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน (authenticator) ตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (authenticator assurance level: AAL)

สารบัญ

สารบัญตาราง

ETDA
สพธอ
www.etda.or.th

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์
ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน

ตามที่สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้ประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน ลงวันที่ ๒๘ กันยายน พ.ศ. ๒๕๖๑ นั้น เนื่องจากมีถ้อยคำที่สมควรแก้ไข จึงให้ยกเลิกประกาศดังกล่าว ทั้งนี้ เพื่อให้มีแนวทางการลงทะเบียน (enrolment) และพิสูจน์ตัวตน (identity proofing) สำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ตามระดับความน่าเชื่อถือของไอเดนทิตี้ (identity assurance level: IAL) ให้เป็นมาตรฐานเดียวกัน

อาศัยอำนาจตามความในมาตรา ๗ (๔) แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. ๒๕๕๔ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) จึงประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน เลขที่ ขมธอ. ๑๙-๒๕๖๑ ปรากฏตามท้ายประกาศฉบับนี้ ทั้งนี้ ตั้งแต่วันที่ ๒๘ กันยายน พ.ศ. ๒๕๖๑ เป็นต้นไป

ประกาศ ณ วันที่ ๑๑ กุมภาพันธ์ พ.ศ. ๒๕๖๒

(นางสุรางคณา วายุภาพ)
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้ เป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการลงทะเบียน (enrolment) และพิสูจน์ตัวตน (identity proofing) ของผู้สมัครใช้บริการที่ประสงค์จะทำธุรกรรมออนไลน์ด้วยดิจิทัลไอดี (digital identity) เพื่อให้ IdP มีแนวทางในการลงทะเบียนและพิสูจน์ตัวตนของผู้สมัครใช้บริการตามระดับความน่าเชื่อถือของไอเดนทิตี (identity assurance level: IAL) ที่เป็นมาตรฐานเดียวกัน

ข้อเสนอแนะมาตรฐานฉบับนี้ อ้างอิงข้อกำหนดเกี่ยวกับการลงทะเบียนและพิสูจน์ตัวตนตามมาตรฐาน NIST Special Publication 800-63A – Digital Identity Guidelines – Enrollment and Identity Proofing ของหน่วยงาน National Institute of Standards and Technology (NIST) เป็นหลัก และนำข้อกำหนดดังกล่าวมาประยุกต์เป็นแนวทางการใช้งานของประเทศไทยที่สอดคล้องกับมาตรฐานสากล

ในข้อเสนอแนะมาตรฐานฉบับนี้ รูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) มีดังต่อไปนี้ [1]

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

2. ระดับความน่าเชื่อถือของไอเดนทิตี (Identity Assurance Level)

ระดับความน่าเชื่อถือของไอเดนทิตี (identity assurance level: IAL) ของผู้ใช้บริการ แบ่งออกเป็น 3 ระดับ ดังนี้

2.1 ระดับ IAL1

ระดับ IAL1 ไม่มีข้อกำหนดในความเชื่อมโยงระหว่างตัวตนของผู้สมัครใช้บริการกับไอเดนทิตีที่มีอยู่ในโลกแห่งความจริง โดยคุณลักษณะใด ๆ ที่ใช้ลงทะเบียนเป็นคุณลักษณะที่ผู้สมัครใช้บริการยืนยันด้วยตนเอง (self-asserted) และไม่มีการตรวจสอบหรือพิสูจน์ความถูกต้องโดย IdP

[1] อ้างอิงข้อมูลจาก ISO/IEC Directives Part 2: Principles and rules for the structure and drafting of ISO and IEC documents

2.2 ระดับ IAL2

ระดับ IAL2 กำหนดให้มีการพิจารณาหลักฐานแสดงตน โดย IdP ต้องตรวจสอบกับ AS ว่าไอเดนทิตีที่กล่าวอ้างมีอยู่ในโลกแห่งความจริง และตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง การพิสูจน์ตัวตนที่ระดับ IAL2 สามารถทำได้ทั้งแบบไม่พบเห็นต่อหน้า หรือแบบพบเห็นต่อหน้า

ทั้งนี้ IdP ที่รองรับระดับ IAL2 สามารถส่งผลการยืนยันตัวตนให้กับ RP ที่ให้บริการธุรกรรมที่ต้องการระดับ IAL1 ได้ หากผู้ใช้บริการให้ความยินยอม (consent)

2.3 ระดับ IAL3

ระดับ IAL3 เพิ่มความเข้มงวดให้กับข้อกำหนดที่ระดับ IAL2 ด้วยการพิจารณาหลักฐานแสดงตนเพิ่มเติม และการตรวจสอบข้อมูลชีวมิติ (biometric) เพื่อป้องกันการปลอมตัวเป็นบุคคลอื่น การหลอกลวง การลงทะเบียนซ้ำ หรือความเสียหายอื่น ๆ การพิสูจน์ตัวตนที่ระดับ IAL3 สามารถทำได้เฉพาะแบบพบเห็นต่อหน้า ซึ่งรวมถึงแบบเสมือนพบเห็นต่อหน้าผ่านช่องทางอิเล็กทรอนิกส์

ทั้งนี้ IdP ที่รองรับระดับ IAL3 สามารถส่งผลการยืนยันตัวตนให้กับ RP ที่ให้บริการธุรกรรมที่ต้องการระดับ IAL1 และ IAL2 ได้ หากผู้ใช้บริการให้ความยินยอม

3. การลงทะเบียนและพิสูจน์ตัวตน

การลงทะเบียนและพิสูจน์ตัวตนมีวัตถุประสงค์เพื่อทำให้มั่นใจว่าผู้สมัครใช้บริการเป็นบุคคลตามที่กล่าวอ้างจริงตามระดับความน่าเชื่อถือที่กำหนด โดยผลลัพธ์ที่คาดว่าจะได้จากการลงทะเบียนและพิสูจน์ตัวตนของผู้สมัครใช้บริการประกอบด้วย

(1) การแยกแยะว่าไอเดนทิตีที่กล่าวอ้างมีเพียงหนึ่งเดียวและมีความเฉพาะเจาะจงภายในบริบทของผู้ใช้บริการทั้งหมดที่ IdP ดูแลอยู่
(2) การตรวจสอบว่าหลักฐานแสดงตนของผู้สมัครใช้บริการเป็นของแท้และข้อมูลมีความถูกต้อง (เช่น ไม่มีการปลอมแปลง หรือใช้งานในทางที่ผิด)
(3) การตรวจสอบว่าไอเดนทิตีที่กล่าวอ้างมีอยู่ในโลกแห่งความจริง
(4) การตรวจสอบตัวบุคคลว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างจริง

การลงทะเบียนและพิสูจน์ตัวตนของผู้สมัครใช้บริการ เริ่มจากการรวบรวมหลักฐานแสดงตนและคุณลักษณะต่าง ๆ จากผู้สมัครใช้บริการ เพื่อให้ได้ไอเดนทิตีที่มีความเฉพาะเจาะจงภายในบริบทหรือกลุ่มผู้ใช้บริการที่กำหนด จากนั้นเป็นการตรวจสอบหลักฐานแสดงตนว่ามีความถูกต้องแท้จริงและสถานะใช้งานได้ และการตรวจสอบตัวบุคคลว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างจริง หลังจากนั้น IdP จะสร้างความเชื่อมโยงระหว่างไอเดนทิตีดังกล่าวกับสิ่งที่ใช้ยืนยันตัวตน (authenticator) เพื่อให้ผู้ใช้บริการใช้ยืนยันตัวตนต่อไป

ทั้งนี้ คุณลักษณะที่จำเป็นในการพิสูจน์ตัวตนอาจมีหลายชุดที่แตกต่างกัน IdP ควรพิจารณาเลือกคุณลักษณะที่รองรับการป้องกันความเป็นส่วนตัวของผู้ใช้บริการและเพียงพอต่อการใช้งานอย่างเหมาะสม รวมถึงพิจารณาคุณลักษณะที่อาจจะจำเป็นสำหรับการใช้งานดิจิทัลไอดีในอนาคตด้วย ตัวอย่างของคุณลักษณะที่จำเป็น เช่น ชื่อเต็ม วันเดือนปีเกิด ที่อยู่ เป็นต้น

การลงทะเบียนและพิสูจน์ตัวตนประกอบด้วย กระบวนการพื้นฐานที่สำคัญ 3 กระบวนการ ดังนี้

3.1 การระบุตัวตน

การระบุตัวตน เป็นกระบวนการที่ IdP รวบรวมคุณลักษณะและหลักฐานแสดงตนที่จำเป็นจากผู้สมัครใช้บริการ เพื่อแยกแยะว่าไอเดนทิตีของผู้สมัครใช้บริการมีเพียงหนึ่งเดียวและมีความเฉพาะเจาะจงภายในบริบทหรือกลุ่มผู้ใช้บริการที่กำหนด ทั้งนี้ การระบุตัวตนที่ดีควรใช้ชุดของคุณลักษณะเท่าที่จำเป็นในการแยกแยะไอเดนทิตีของผู้สมัครใช้บริการแต่ละราย

3.2 การตรวจสอบหลักฐานแสดงตน

การตรวจสอบหลักฐานแสดงตน เป็นกระบวนการที่ IdP ตรวจสอบความแท้จริง (authenticity) สถานะการใช้งาน (validity) และความถูกต้อง (accuracy) ของหลักฐานแสดงตน และตรวจสอบข้อมูลที่อยู่ในหลักฐานแสดงตนว่าเป็นของบุคคลที่มีตัวตนอยู่จริง รวมถึงตรวจสอบช่องทางการติดต่อว่าสามารถใช้ติดต่อได้

3.3 การตรวจสอบตัวบุคคล

การตรวจสอบตัวบุคคล เป็นกระบวนการที่ IdP ตรวจสอบตัวบุคคลที่แสดงหลักฐานแสดงตนว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง

4. ข้อกำหนดเกี่ยวกับการลงทะเบียนและพิสูจน์ตัวตน

ข้อกำหนดเกี่ยวกับการลงทะเบียนและพิสูจน์ตัวตนมีจุดมุ่งหมายเพื่อให้มั่นใจว่าไอเดนทิตีที่กล่าวอ้างเป็นไอเดนทิตีของผู้สมัครใช้บริการจริง

4.1 ข้อกำหนดทั่วไป (ที่ระดับ IAL2 และ IAL3)

ข้อกำหนดต่อไปนี้ใช้สำหรับ IdP ในการพิสูจน์ตัวตนที่ระดับ IAL2 และ IAL3

(1) การรวบรวมข้อมูลระบุตัวบุคคล (personally identifiable information) ต้องเป็นคุณลักษณะเท่าที่จำเป็นต่อการตรวจสอบว่าไอเดนทิตีที่กล่าวอ้างมีอยู่ในโลกแห่งความจริงและผู้สมัครใช้บริการเป็นเจ้าของไอเดนทิตีดังกล่าว ทั้งนี้ อาจรวมถึงคุณลักษณะที่ใช้ตรวจสอบหลักฐานแสดงตนกับ AS และคุณลักษณะที่ส่งให้กับ RP เพื่อใช้พิจารณากำหนดสิทธิของผู้ใช้บริการ

(2) IdP ต้องแจ้งให้ผู้สมัครใช้บริการทราบอย่างชัดเจนเกี่ยวกับวัตถุประสงค์ในการรวบรวมและจัดเก็บคุณลักษณะที่ใช้สำหรับการพิสูจน์ตัวตน รวมถึงระบุว่าคุณลักษณะใดเป็นคุณลักษณะที่ขึ้นอยู่กับความสมัครใจหรือคุณลักษณะใดเป็นคุณลักษณะที่จำเป็น พร้อมกับผลที่ตามมาหากผู้สมัครใช้บริการไม่แสดงคุณลักษณะดังกล่าวกับ IdP

(3) IdP ต้องไม่นำคุณลักษณะที่รวบรวมและจัดเก็บในกระบวนการพิสูจน์ตัวตนไปใช้กับวัตถุประสงค์อื่นนอกเหนือจากการพิสูจน์ตัวตน การยืนยันตัวตน หรือตามที่กฎหมายกำหนด เว้นแต่ IdP ได้แจ้งให้ผู้สมัครใช้บริการทราบอย่างชัดเจนและได้รับความยินยอมให้นำคุณลักษณะไปใช้กับวัตถุประสงค์อื่น ๆ ทั้งนี้ IdP ต้องไม่กำหนดการให้ความยินยอมให้นำคุณลักษณะไปใช้กับวัตถุประสงค์อื่น ๆ เป็นเงื่อนไขในการให้บริการ

(4) IdP ต้องมีกลไกแก้ไขข้อร้องเรียนหรือปัญหาของผู้สมัครใช้บริการที่เกิดขึ้นจากการพิสูจน์ตัวตน โดยกลไกดังกล่าวต้องง่ายต่อการค้นหาและง่ายต่อการใช้งานของผู้สมัครใช้บริการ ทั้งนี้ IdP ต้องประเมินประสิทธิภาพของกลไกต่าง ๆ ในการแก้ไขข้อร้องเรียนหรือปัญหาที่เกิดขึ้น

(5) IdP ต้องจัดทำแนวนโยบายหรือแนวปฏิบัติของการลงทะเบียนและพิสูจน์ตัวตน และต้องดำเนินการลงทะเบียนและพิสูจน์ตัวตนตามขั้นตอนที่ระบุไว้ในแนวนโยบายหรือแนวปฏิบัติดังกล่าว ทั้งนี้ แนวปฏิบัติต้องประกอบด้วยมาตรการควบคุมที่อธิบายการรับมือข้อผิดพลาดในการพิสูจน์ตัวตนซึ่งทำให้การลงทะเบียนของผู้สมัครใช้บริการไม่เป็นผลสำเร็จ เช่น จำนวนครั้งที่อนุญาตให้ทดลองใหม่ ทางเลือกในการพิสูจน์ตัวตนกรณีที่ระบบออนไลน์ขัดข้อง หรือมาตรการรับมือการทุจริตเมื่อตรวจพบความผิดปกติ เป็นต้น

(6) IdP ต้องจัดเก็บบันทึกรายละเอียดของการพิสูจน์ตัวตน รวมถึงบันทึกการตรวจสอบ (audit log) ของขั้นตอนทั้งหมดที่ใช้พิสูจน์ตัวตนของผู้สมัครใช้บริการ และต้องบันทึกประเภทของหลักฐานแสดงตนที่ผู้สมัครใช้บริการแสดงในกระบวนการพิสูจน์ตัวตน นอกจากนี้ IdP ต้องดำเนินการบริหารความเสี่ยง ซึ่งรวมถึงการประเมินความเสี่ยงด้านความเป็นส่วนตัวและความมั่นคงปลอดภัยเพื่อกำหนด

ก. ขั้นตอนเพิ่มเติมใด ๆ ที่ใช้พิสูจน์ตัวตนของผู้สมัครใช้บริการนอกเหนือจากข้อกำหนดที่ต้องปฏิบัติตามซึ่งระบุไว้ในข้อเสนอแนะมาตรฐานฉบับนี้

ข. ข้อมูลระบุตัวบุคคล รวมถึงข้อมูลชีวมิติ (biometric) ภาพ ภาพสแกน หรือสำเนาของหลักฐานแสดงตนอื่น ๆ ซึ่ง IdP จะจัดเก็บไว้เพื่อเป็นบันทึกรายละเอียดของการพิสูจน์ตัวตน

ค. ระยะเวลาการเก็บรักษาบันทึกรายละเอียดของการพิสูจน์ตัวตนตามกฎหมาย ข้อบังคับ หรือแนวนโยบายที่เกี่ยวข้อง

(7) ข้อมูลระบุตัวบุคคลทั้งหมดที่รวบรวมในกระบวนการลงทะเบียนและพิสูจน์ตัวตนต้องมีการปกป้องเพื่อให้มีการรักษาความลับ (confidentiality) การรักษาความครบถ้วน (integrity) และการระบุแหล่งที่มาของข้อมูล (attribution of information source)

(8) ธุรกรรมเกี่ยวกับการพิสูจน์ตัวตนทั้งหมด รวมถึงธุรกรรมที่เกี่ยวข้องกับบุคคลที่สามต้องดำเนินการผ่านช่องทางการติดต่อสื่อสารที่มีความมั่นคงปลอดภัยและน่าเชื่อถือ

(9) IdP ควรมีมาตรการเพิ่มเติมเพื่อป้องกันการทุจริตและเพิ่มความน่าเชื่อถือในการพิสูจน์ตัวตน เช่น การตรวจสอบตำแหน่งทางภูมิศาสตร์ การตรวจสอบลักษณะอุปกรณ์ของผู้สมัครใช้บริการ การประเมินลักษณะพฤติกรรมของผู้สมัครใช้บริการ เป็นต้น โดย IdP ต้องประเมินความเสี่ยงด้านความเป็นส่วนตัวของผู้สมัครใช้บริการจากการใช้มาตรการป้องกันการทุจริตดังกล่าว

(10) ในกรณีที่ IdP ยุติการดำเนินการลงทะเบียนและพิสูจน์ตัวตน IdP ต้องรับผิดชอบในการกำจัดหรือทำลายข้อมูลที่อ่อนไหว (sensitive data) รวมถึงข้อมูลระบุตัวบุคคล หรือการป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตตลอดระยะเวลาการเก็บรักษา

4.2 ข้อกำหนดของการแสดงตน

ข้อกำหนดของการแสดงตนของผู้สมัครใช้บริการ สามารถแสดงได้ตามตารางที่ 1

ตารางที่ 1 ข้อกำหนดของการแสดงตน

ระดับความน่าเชื่อถือ	ข้อกำหนดของการแสดงตน
IAL1	ไม่มีข้อกำหนด
IAL2	IdP รองรับการพิสูจน์ตัวตน – แบบไม่พบเห็นต่อหน้า **หรือ** – แบบพบเห็นต่อหน้า
IAL3	IdP รองรับการพิสูจน์ตัวตน – แบบพบเห็นต่อหน้า โดยปฏิบัติตามข้อกำหนดในหัวข้อ 4.2.1 **หรือ** – แบบเสมือนพบเห็นต่อหน้าผ่านช่องทางอิเล็กทรอนิกส์ โดยปฏิบัติตามข้อกำหนดในหัวข้อ 4.2.1 และ 4.2.2

4.2.1 ข้อกำหนดของการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า (ที่ระดับ IAL3)

(1) IdP ต้องมีเจ้าหน้าที่ทำหน้าที่สังเกตสิ่งผิดปกติบนร่างกายของผู้สมัครใช้บริการ (เช่น ใบหน้า นิ้วมือ) และดำเนินการตรวจสอบตามกระบวนการพิสูจน์ตัวตน

(2) IdP ต้องรวบรวมข้อมูลชีวมิติในลักษณะที่มั่นใจว่า ข้อมูลชีวมิติดังกล่าวถูกรวบรวมจากผู้สมัครใช้บริการ และไม่ใช่จากบุคคลอื่น

4.2.2 ข้อกำหนดของการพิสูจน์ตัวตนแบบเสมือนพบเห็นต่อหน้าผ่านช่องทางอิเล็กทรอนิกส์ (ที่ระดับ IAL3)

IdP สามารถใช้การพิสูจน์ตัวตนแบบเสมือนพบเห็นต่อหน้าผ่านช่องทางอิเล็กทรอนิกส์ เพื่อให้ได้ความน่าเชื่อถือและความมั่นคงปลอดภัยในระดับเดียวกันกับการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า โดยการพิสูจน์ตัวตนแบบเสมือนพบเห็นต่อหน้าผ่านช่องทางอิเล็กทรอนิกส์ ต้องเป็นไปตามข้อกำหนดต่อไปนี้

(1) IdP ต้องเฝ้าสังเกตผู้สมัครใช้บริการตลอดเวลาของการพิสูจน์ตัวตน โดยที่ผู้สมัครใช้บริการต้องไม่ออกไปจากการสื่อสาร ตัวอย่างเช่น การเฝ้าสังเกตผู้สมัครใช้บริการด้วยการส่งผ่านวิดีโอที่มีความละเอียดสูงอย่างต่อเนื่อง

(2) IdP ต้องมีเจ้าหน้าที่เข้าร่วมการสนทนาออนไลน์กับผู้สมัครใช้บริการแบบถ่ายทอดสดตลอดเวลาของการพิสูจน์ตัวตน

(3) เจ้าหน้าที่ต้องสามารถมองเห็นพฤติกรรมทั้งหมดของผู้สมัครใช้บริการระหว่างช่วงเวลาของการพิสูจน์ตัวตนได้อย่างชัดเจน

(4) IdP ต้องตรวจสอบหลักฐานแสดงตนด้วยวิธีการทางอิเล็กทรอนิกส์ (เช่น การอ่านข้อมูลผ่านชิป (chip) หรือเทคโนโลยีไร้สาย) โดยใช้เครื่องมืออุปกรณ์ของ IdP ทั้งหมด

(5) IdP ต้องฝึกอบรมเจ้าหน้าที่เพื่อให้สามารถตรวจหาความผิดปกติที่อาจเกิดขึ้นในการพิสูจน์ตัวตนและดำเนินการได้อย่างเหมาะสม

(6) IdP ต้องติดตั้งระบบตรวจจับการบุกรุกทางกายภาพที่เหมาะสมกับสภาพแวดล้อมของสถานที่ตั้ง ตัวอย่างเช่น เครื่องให้บริการ (kiosk) ที่ตั้งอยู่ในพื้นที่ที่จำกัดหรือพื้นที่ที่มีการรักษาความมั่นคงปลอดภัยจะมีระบบการตรวจจับการบุกรุกที่น้อยกว่าเครื่องให้บริการที่ตั้งอยู่ในพื้นที่กึ่งสาธารณะ เช่น ห้างสรรพสินค้า

(7) IdP ต้องตรวจสอบให้มั่นใจว่าการติดต่อสื่อสารทั้งหมดเกิดขึ้นผ่านช่องทางการสื่อสารเฉพาะที่มีการป้องกัน

4.3 ข้อกำหนดของการระบุตัวตน

ข้อกำหนดของการระบุตัวตนของผู้สมัครใช้บริการสามารถแสดงได้ตามตารางที่ 2

ตารางที่ 2 ข้อกำหนดของการระบุตัวตน

ระดับความน่าเชื่อถือ	ข้อกำหนดของการระบุตัวตน
IAL1	ไม่มีข้อกำหนด
IAL2	– IdP ต้องรวบรวมข้อมูลระบุตัวบุคคล โดยเป็นคุณลักษณะเท่าที่จำเป็นสำหรับใช้แยกแยะว่าไอเดนทิตีมีเพียงหนึ่งเดียวและมีความเฉพาะเจาะจงภายในบริบทที่กำหนด – IdP อาจใช้วิธีการที่เหมาะสมในการพิจารณาความแตกต่างของข้อมูลส่วนบุคคลและข้อมูลที่เกี่ยวข้องจากหลักฐานแสดงตนและ AS ทั้งนี้ IdP ควรเผยแพร่วิธีการและหลักเกณฑ์ที่ใช้เปรียบเทียบต่อสาธารณะหรือผู้ที่เกี่ยวข้อง ซึ่งอาจรวมไว้ในแนวนโยบายหรือแนวปฏิบัติของการลงทะเบียนและพิสูจน์ตัวตน – IdP อาจใช้การยืนยันด้วยชุดข้อมูลที่รู้เฉพาะผู้สมัครใช้บริการ (knowledge-based verification: KBV) เปรียบเทียบกับข้อมูลที่ได้จาก AS
IAL3	ข้อกำหนดเช่นเดียวกับ IAL2

4.4 ข้อกำหนดของการตรวจสอบหลักฐานแสดงตน

ข้อกำหนดของการตรวจสอบหลักฐานแสดงตนจากผู้สมัครใช้บริการ สามารถแสดงได้ตามตารางที่ 3

ตารางที่ 3 ข้อกำหนดของการตรวจสอบหลักฐานแสดงตน

ระดับความน่าเชื่อถือ	ข้อกำหนดของการตรวจสอบหลักฐานแสดงตน
IAL1	ไม่มีข้อกำหนด
IAL2	– IdP ต้องขอหลักฐานแสดงตนจากผู้สมัครใช้บริการ คือ บัตรประจำตัวประชาชน **หรือ** หนังสือเดินทาง ที่ยังไม่หมดอายุ – IdP ต้องตรวจสอบหลักฐานแสดงตนว่าเป็นของแท้ โดยใช้เจ้าหน้าที่**หรือ**เทคโนโลยีที่เหมาะสม – IdP ต้องตรวจสอบข้อมูลของผู้สมัครใช้บริการจากหลักฐานแสดงตนว่ามีความถูกต้องโดยเปรียบเทียบกับข้อมูลจาก AS
IAL3	– IdP ต้องขอหลักฐานแสดงตนจากผู้สมัครใช้บริการ คือ บัตรประจำตัวประชาชน **และ** หนังสือเดินทาง ที่ยังไม่หมดอายุ – IdP ต้องตรวจสอบหลักฐานแสดงตนว่าเป็นของแท้ โดยใช้เจ้าหน้าที่**และ**เทคโนโลยีที่เหมาะสม

ระดับความน่าเชื่อถือ	ข้อกำหนดของการตรวจสอบหลักฐานแสดงตน
	– IdP ต้องตรวจสอบข้อมูลของผู้สมัครใช้บริการจากหลักฐานแสดงตนว่ามีความถูกต้อง โดยเปรียบเทียบกับข้อมูลจาก AS

4.5 ข้อกำหนดของการตรวจสอบตัวบุคคล

ข้อกำหนดของการตรวจสอบตัวบุคคลของผู้สมัครใช้บริการ สามารถแสดงได้ตามตารางที่ 4

ตารางที่ 4 ข้อกำหนดของการตรวจสอบตัวบุคคล

ระดับความน่าเชื่อถือ	ข้อกำหนดของการตรวจสอบตัวบุคคล
IAL1	ไม่มีข้อกำหนด
IAL2	– IdP ต้องตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง โดย ● เปรียบเทียบลักษณะที่ปรากฏของผู้สมัครใช้บริการกับรูปถ่ายจากหลักฐานแสดงตน (physical comparison) **หรือ** ● เปรียบเทียบข้อมูลชีวมิติของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison) – IdP อาจบันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (biometric sample) (เช่น ภาพใบหน้า ลายนิ้วมือ) เพื่อวัตถุประสงค์ในการห้ามปฏิเสธความรับผิด (non-repudiation) และการตรวจสอบอีกครั้งกรณีจำเป็น (re-proofing)
IAL3	– IdP ต้องตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง โดยเปรียบเทียบข้อมูลชีวมิติของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison) – IdP ต้องบันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (biometric sample) (เช่น ภาพใบหน้า ลายนิ้วมือ) เพื่อวัตถุประสงค์ในการห้ามปฏิเสธความรับผิด (non-repudiation) และการตรวจสอบอีกครั้งกรณีจำเป็น (re-proofing)

4.6 ข้อกำหนดของการตรวจสอบช่องทางการติดต่อ

ข้อกำหนดของการตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการ สามารถแสดงได้ตามตารางที่ 5

ตารางที่ 5 ข้อกำหนดของการตรวจสอบช่องทางการติดต่อ

ระดับความน่าเชื่อถือ	ข้อกำหนดของการตรวจสอบช่องทางการติดต่อ
IAL1	ไม่มีข้อกำหนด
IAL2	IdP ต้องตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง เช่น – การตรวจสอบอีเมลด้วยวิธีการยืนยันทางอีเมล – การตรวจสอบหมายเลขโทรศัพท์มือถือด้วยรหัสผ่านแบบใช้ครั้งเดียว (OTP) หรือวิธีการยืนยันทาง SMS
IAL3	ข้อกำหนดเช่นเดียวกับ IAL2

4.7 สรุปข้อกำหนดตามระดับ IAL

ข้อกำหนดตามระดับ IAL แต่ละระดับ สามารถสรุปได้ตามตารางที่ 6

ตารางที่ 6 สรุปข้อกำหนดตามระดับ IAL

ข้อกำหนด	IAL1	IAL2	IAL3
การแสดงตน	ไม่มีข้อกำหนด	– แบบไม่พบเห็นต่อหน้า **หรือ** – แบบพบเห็นต่อหน้า	– แบบพบเห็นต่อหน้า โดยปฏิบัติตามข้อกำหนดในหัวข้อ 4.2.1 **หรือ** – แบบเสมือนพบเห็นต่อหน้าผ่านช่องทางอิเล็กทรอนิกส์ โดยปฏิบัติตามข้อกำหนดในหัวข้อ 4.2.1 และ 4.2.2
การระบุตัวตน	ไม่มีข้อกำหนด	– ต้องรวบรวมข้อมูลระบุตัวบุคคลโดยเป็นคุณลักษณะเท่าที่จำเป็นสำหรับใช้แยกแยะว่าไอเดนทิตีมีเพียงหนึ่งเดียวและมีความเฉพาะเจาะจงภายในบริบทที่กำหนด – อาจใช้วิธีการที่เหมาะสมในการพิจารณาความแตกต่างของข้อมูลส่วนบุคคลและข้อมูลที่เกี่ยวข้องจากหลักฐานแสดงตนและ AS – อาจใช้การยืนยันด้วยชุดข้อมูลที่รู้เฉพาะผู้สมัครใช้บริการ (KBV) เปรียบเทียบกับข้อมูลที่ได้จาก AS	ข้อกำหนดเช่นเดียวกับ IAL2
การตรวจสอบหลักฐานแสดงตน	ไม่มีข้อกำหนด	– หลักฐานแสดงตนจากผู้สมัครใช้บริการ คือ บัตรประจำตัวประชาชน **หรือ** หนังสือเดินทาง ที่ยังไม่หมดอายุ – ต้องตรวจสอบหลักฐานแสดงตนว่าเป็นของแท้ โดยใช้เจ้าหน้าที่**หรือ**เทคโนโลยีที่เหมาะสม – ต้องตรวจสอบข้อมูลของผู้สมัครใช้บริการจากหลักฐานแสดงตนว่ามีความถูกต้องโดยเปรียบเทียบกับข้อมูลจาก AS	– หลักฐานแสดงตนจากผู้สมัครใช้บริการ คือ บัตรประจำตัวประชาชน **และ** หนังสือเดินทาง ที่ยังไม่หมดอายุ – ต้องตรวจสอบหลักฐานแสดงตนว่าเป็นของแท้ โดยใช้เจ้าหน้าที่**และ**เทคโนโลยีที่เหมาะสม – ต้องตรวจสอบข้อมูลของผู้สมัครใช้บริการจากหลักฐานแสดงตนว่ามีความถูกต้องโดยเปรียบเทียบกับข้อมูลจาก AS
การตรวจสอบตัวบุคคล	ไม่มีข้อกำหนด	– ต้องตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง โดย ● เปรียบเทียบลักษณะที่ปรากฏของผู้สมัครใช้บริการกับรูปถ่ายจากหลักฐานแสดงตน (physical comparison) **หรือ**	– ต้องตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง โดยเปรียบเทียบข้อมูลชีวมิติของผู้สมัครใช้บริการกับข้อมูลจากหลักฐานแสดงตน (biometric comparison)

ข้อกำหนด	IAL1	IAL2	IAL3
		● เปรียบเทียบข้อมูลชีวมิติของผู้สมัครใช้บริการกับข้อมูลจากหลักฐานแสดงตน (biometric comparison) – อาจบันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (biometric sample) (เช่น ภาพใบหน้า ลายนิ้วมือ)	– ต้องบันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (biometric sample) (เช่น ภาพใบหน้า ลายนิ้วมือ)
การตรวจสอบช่องทางการติดต่อ	ไม่มีข้อกำหนด	ต้องตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง	ข้อกำหนดเช่นเดียวกับ IAL2

5. แนวทางการกำหนดระดับ IAL ของประเทศไทย

แนวทางการกำหนดระดับ IAL ของประเทศไทย ที่มีการแบ่งระดับ IAL1 และ IAL2 ออกเป็น 3 ระดับย่อย ได้แก่ ระดับ IAL1.1, IAL1.2, IAL1.3, IAL2.1, IAL2.2 และ IAL2.3 สามารถแสดงได้ตามตารางที่ 7

ตารางที่ 7 แนวทางการกำหนดระดับ IAL ของประเทศไทย

ระดับความน่าเชื่อถือ	การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า	การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า ผ่านเครื่องให้บริการ (kiosk) ของ IdP	การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า ผ่านแอปพลิเคชัน (application) ของ IdP
IAL1.1	ไม่มีข้อกำหนด	ไม่มีข้อกำหนด	ไม่มีข้อกำหนด
IAL1.2	การระบุตัวตน – รวบรวมข้อมูลระบุตัวบุคคล การตรวจสอบหลักฐานแสดงตน – สำเนาบัตรประจำตัวประชาชน**หรือ**สำเนาหนังสือเดินทาง ที่ยังไม่หมดอายุ พร้อมรับรองสำเนาถูกต้อง	การระบุตัวตน – รวบรวมข้อมูลระบุตัวบุคคล การตรวจสอบหลักฐานแสดงตน – รูปบัตรประจำตัวประชาชน**หรือ**รูปหนังสือเดินทาง ที่ยังไม่หมดอายุ	การระบุตัวตน – รวบรวมข้อมูลระบุตัวบุคคล การตรวจสอบหลักฐานแสดงตน – รูปบัตรประจำตัวประชาชน**หรือ**รูปหนังสือเดินทาง ที่ยังไม่หมดอายุ
IAL1.3	การระบุตัวตน – รวบรวมข้อมูลระบุตัวบุคคล การตรวจสอบหลักฐานแสดงตน – บัตรประจำตัวประชาชน**หรือ**หนังสือเดินทาง ที่ยังไม่หมดอายุ – เจ้าหน้าที่ดูหลักฐานแสดงตน เพื่อตรวจสอบว่าเป็นของแท้ – เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลบนหลักฐานแสดงตน เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง	การระบุตัวตน – รวบรวมข้อมูลระบุตัวบุคคล การตรวจสอบหลักฐานแสดงตน – บัตรประจำตัวประชาชน**หรือ**หนังสือเดินทาง ที่ยังไม่หมดอายุ – ผู้สมัครใช้บริการถ่ายรูปหลักฐานแสดงตนที่เครื่องให้บริการของ IdP และเจ้าหน้าที่ดูรูปหลักฐานแสดงตน เพื่อตรวจสอบว่าเป็นของแท้ – เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลบนหลักฐานแสดงตน เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง	การระบุตัวตน – รวบรวมข้อมูลระบุตัวบุคคล การตรวจสอบหลักฐานแสดงตน – บัตรประจำตัวประชาชน**หรือ**หนังสือเดินทาง ที่ยังไม่หมดอายุ – ผู้สมัครใช้บริการถ่ายรูปหลักฐานแสดงตนผ่านแอปพลิเคชันของ IdP และเจ้าหน้าที่ดูรูปหลักฐานแสดงตน เพื่อตรวจสอบว่าเป็นของแท้ – เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลบนหลักฐานแสดงตน เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง
IAL2.1	การระบุตัวตน – รวบรวมข้อมูลระบุตัวบุคคล การตรวจสอบหลักฐานแสดงตน – บัตรประจำตัวประชาชน**หรือ**หนังสือเดินทาง ที่ยังไม่หมดอายุ – เจ้าหน้าที่ใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์ เพื่อตรวจสอบหลักฐานแสดงตนว่าเป็นของแท้	การระบุตัวตน – รวบรวมข้อมูลระบุตัวบุคคล การตรวจสอบหลักฐานแสดงตน – บัตรประจำตัวประชาชน**หรือ**หนังสือเดินทาง ที่ยังไม่หมดอายุ – ผู้สมัครใช้บริการใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์ที่เครื่องให้บริการของ IdP เพื่อตรวจสอบหลักฐาน	การระบุตัวตน – รวบรวมข้อมูลระบุตัวบุคคล การตรวจสอบหลักฐานแสดงตน – บัตรประจำตัวประชาชน**หรือ**หนังสือเดินทาง ที่ยังไม่หมดอายุ – ผู้สมัครใช้บริการใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์หรือเทคโนโลยีที่กำหนด เพื่อตรวจสอบหลักฐานแสดงตน

ระดับความน่าเชื่อถือ	การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า	การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า ผ่านเครื่องให้บริการ (kiosk) ของ IdP	การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า ผ่านแอปพลิเคชัน (application) ของ IdP
	– เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง <u>การตรวจสอบตัวบุคคล</u> – เจ้าหน้าที่อาจถ่ายรูปและบันทึกภาพใบหน้าของผู้สมัครใช้บริการ เพื่อใช้เป็นหลักฐาน – เจ้าหน้าที่เปรียบเทียบลักษณะที่ปรากฏของผู้สมัครใช้บริการกับรูปถ่ายจากหลักฐานแสดงตน (physical comparison) <u>การตรวจสอบช่องทางการติดต่อ</u> – ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง	แสดงตนว่าเป็นของแท้ – IdP เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง <u>การตรวจสอบตัวบุคคล</u> – ผู้สมัครใช้บริการถ่ายรูปตัวเองที่เครื่องให้บริการของ IdP และ IdP บันทึกภาพใบหน้าของผู้สมัครใช้บริการเพื่อใช้เป็นหลักฐาน – เจ้าหน้าที่เปรียบเทียบรูปถ่ายของผู้สมัครใช้บริการกับรูปถ่ายจากหลักฐานแสดงตน (physical comparison) <u>การตรวจสอบช่องทางการติดต่อ</u> – ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง	ว่าเป็นของแท้ – IdP เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง <u>การตรวจสอบตัวบุคคล</u> – ผู้สมัครใช้บริการถ่ายรูปตัวเองพร้อมหลักฐานแสดงตนผ่านแอปพลิเคชันของ IdP และ IdP บันทึกภาพใบหน้าของผู้สมัครใช้บริการ เพื่อใช้เป็นหลักฐาน – เจ้าหน้าที่เปรียบเทียบรูปถ่ายของผู้สมัครใช้บริการกับรูปถ่ายจากหลักฐานแสดงตน (physical comparison) <u>การตรวจสอบช่องทางการติดต่อ</u> – ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง
IAL2.2	ข้อกำหนดทั้งหมดเช่นเดียวกับ IAL2.1 โดยเพิ่มเติม <u>การตรวจสอบหลักฐานแสดงตน</u> – ใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์ ตรวจสอบหลักฐานแสดงตนออนไลน์กับ AS <u>การตรวจสอบตัวบุคคล</u> – เจ้าหน้าที่ถ่ายรูปและบันทึกภาพใบหน้าของผู้สมัครใช้บริการ เพื่อใช้เป็นหลักฐาน	ข้อกำหนดทั้งหมดเช่นเดียวกับ IAL2.1 โดยเพิ่มเติม <u>การตรวจสอบหลักฐานแสดงตน</u> – ใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์ ตรวจสอบหลักฐานแสดงตนออนไลน์กับ AS	ข้อกำหนดทั้งหมดเช่นเดียวกับ IAL2.1 โดยเพิ่มเติม <u>การตรวจสอบหลักฐานแสดงตน</u> – ใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์หรือเทคโนโลยีที่กำหนด ตรวจสอบหลักฐานแสดงตนออนไลน์กับ AS
IAL2.3	ข้อกำหนดทั้งหมดเช่นเดียวกับ IAL2.2 โดยเพิ่มเติม <u>การตรวจสอบตัวบุคคล</u> – ใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)	ข้อกำหนดทั้งหมด เช่นเดียวกับ IAL2.2 โดยเพิ่มเติม <u>การตรวจสอบตัวบุคคล</u> – ใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)	ข้อกำหนดทั้งหมดเช่นเดียวกับ IAL2.2 โดยเพิ่มเติม <u>การตรวจสอบตัวบุคคล</u> – ใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)

ระดับความน่าเชื่อถือ	การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า	การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า ผ่านเครื่องให้บริการ (kiosk) ของ IdP	การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า ผ่านแอปพลิเคชัน (application) ของ IdP
IAL3	<u>การแสดงตน</u> – พบเห็นต่อหน้า (ตามข้อกำหนดในหัวข้อ 4.2.1) <u>การระบุตัวตน</u> – รวบรวมข้อมูลระบุตัวบุคคล <u>การตรวจสอบหลักฐานแสดงตน</u> – บัตรประจำตัวประชาชน**และ**หนังสือเดินทาง ที่ยังไม่หมดอายุ – เจ้าหน้าที่ดูหลักฐานแสดงตน และใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์ เพื่อตรวจสอบว่าเป็นของแท้ – เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง <u>การตรวจสอบตัวบุคคล</u> – เจ้าหน้าที่บันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (biometric sample) เช่น ภาพใบหน้า ลายนิ้วมือ – ใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison) <u>การตรวจสอบช่องทางการติดต่อ</u> – ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง	<u>การแสดงตน</u> – เสมือนพบเห็นต่อหน้าผ่านช่องทางอิเล็กทรอนิกส์ (ตามข้อกำหนดในหัวข้อ 4.2.1 และ 4.2.2) <u>การระบุตัวตน</u> – รวบรวมข้อมูลระบุตัวบุคคล <u>การตรวจสอบหลักฐานแสดงตน</u> – บัตรประจำตัวประชาชน**และ**หนังสือเดินทาง ที่ยังไม่หมดอายุ – เจ้าหน้าที่ดูหลักฐานแสดงตน และผู้สมัครใช้บริการใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์ เพื่อตรวจสอบว่าเป็นของแท้ – IdP เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง <u>การตรวจสอบตัวบุคคล</u> – IdP บันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (biometric sample) เช่น ภาพใบหน้า ลายนิ้วมือ – ใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison) <u>การตรวจสอบช่องทางการติดต่อ</u> – ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง	

ภาคผนวก ก.
ความสัมพันธ์ระหว่างระดับ IAL ของประเทศไทยกับมาตรฐานการพิสูจน์ตัวตนอื่น ๆ

ข้อเสนอแนะมาตรฐานฉบับนี้มีจุดมุ่งหมายเพื่อให้ข้อกำหนดตามระดับ IAL ของประเทศไทยมีความสอดคล้องกับมาตรฐานระดับประเทศและระดับสากลที่กำหนดระดับของการพิสูจน์ตัวตน โดยความสัมพันธ์กับมาตรฐานการพิสูจน์ตัวตนระดับประเทศและระดับสากลต่าง ๆ สามารถแสดงได้ตามตารางที่ 8 อย่างไรก็ตาม ตารางนี้ไม่ได้หมายความถึงความสัมพันธ์โดยตรงระหว่างระดับ IAL ในข้อเสนอแนะมาตรฐานฉบับนี้กับระดับของการพิสูจน์ตัวตนในมาตรฐานระดับประเทศและระดับสากลเหล่านั้น แต่ข้อกำหนดตามระดับ IAL ในข้อเสนอแนะมาตรฐานฉบับนี้สามารถถือได้ว่ามีคุณสมบัติตรงตามหลักเกณฑ์ที่อธิบายไว้ในมาตรฐานเหล่านั้น

ตารางที่ 8 ความสัมพันธ์ระหว่างระดับ IAL ของประเทศไทยกับมาตรฐานการพิสูจน์ตัวตนอื่น ๆ

ชื่อมาตรฐาน	ระดับความน่าเชื่อถือ			
ISO/IEC 29115:2013 – Information technology – Security techniques – Entity authentication assurance framework	LOA 1	LOA 2	LOA 3	LOA 4
ข้อเสนอแนะมาตรฐานฯ แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน	**IAL 1**	**IAL 1**	**IAL 2**	**IAL 3**
NIST Special Publication 800-63A – Digital Identity Guidelines – Enrollment and Identity Proofing, June 2017	IAL 1	IAL 1	IAL 2	IAL 3
UK Government - Good Practice Guide No. 45 – Identity Proofing and Verification of an Individual, Issue No: 2.3, July 2014	Level 1	Level 2	Level 3	Level 4
Australian Government - Trusted Digital Identity Framework – Identity Proofing Requirements, version 1.0, February 2018	IP 1	IP 2	IP 3	IP 4