สพร. / CDV
สิงหาคม ๒๕๖๓

มาตรฐานรัฐบาลดิจิทัลอยู่ระหว่างการจัดทำ
ห้ามใช้หรือยึดร่างนี้เป็นมาตรฐาน

มาตรฐานรัฐบาลดิจิทัลฉบับสมบูรณ์จะมีประกาศโดย
คณะกรรมการพัฒนารัฐบาลดิจิทัล

ร่าง

มาตรฐานรัฐบาลดิจิทัล
Digital Government Standard

ว่าด้วย แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

DIGITALIZATION: DIGITAL ID – IDENTITY PROOFING AND AUTHENTICATION

สำหรับเวียนขอข้อคิดเห็นจากหน่วยงานต่าง ๆ ที่เกี่ยวข้อง

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ชั้น ๑๗ อาคารบางกอกไทยทาวเวอร์ ๑๐๘ ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ ๑๐๔๐๐
หมายเลขโทรศัพท์: (+๖๖) ๐ ๒๖๑๒ ๖๐๐๐ โทรสาร: (+๖๖) ๐ ๒๖๑๒ ๖๐๑๑ (+๖๖) ๐ ๒๖๑๒ ๖๐๑๒

สารบัญ

สารบัญตาราง

สารบัญภาพ

คำนำ

การจัดทำกระบวนการและการดำเนินงานทางดิจิทัลของภาครัฐ เป็นการวางรูปแบบร่วมกันเพื่อสร้างขั้นตอนการทำงาน พัฒนาบริการให้เป็นรูปแบบดิจิทัลแบบครบวงจร สามารถเชื่อมโยงข้อมูลระหว่างหน่วยงานได้ โดยมีการนำระบบเทคโนโลยีดิจิทัลมาใช้ในการทำงาน เป็นกลไกในการเพิ่มประสิทธิภาพในการให้บริการภาครัฐแก่ประชาชน เป็นการเพิ่มทางเลือกให้แก่ประชาชนในการขอรับบริการจากภาครัฐ ช่วยลดความผิดพลาด ยกระดับการทำงานของภาครัฐผ่านระบบดิจิทัลตั้งแต่ต้นจนจบได้อย่างสมบูรณ์ นำไปสู่การเป็นรัฐบาลดิจิทัลที่ไร้กระดาษ (Paperless) ซึ่งกระบวนการหลักของการดำเนินงานทางดิจิทัลของภาครัฐเริ่มตั้งแต่การพิสูจน์และยืนยันตัวตนทางดิจิทัลไปจนถึงการจัดส่งใบอนุญาตหรือเอกสารต่าง ๆ ทางดิจิทัล

การพิสูจน์และยืนยันตัวตนทางดิจิทัล เป็นกระบวนการแรกที่สำคัญในการเข้าสู่บริการภาครัฐ ซึ่งหน่วยงานของรัฐต้องประเมินความต้องการของหน่วยงานเพื่อพิจารณาว่าบริการใดบ้างที่จำเป็นต้องใช้ดิจิทัลไอดีในการพิสูจน์และยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐ โดยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัลที่เกี่ยวกับแนวทางการใช้ดิจิทัลไอดีสำหรับหน่วยงานของรัฐ ประกอบด้วย

(๑) แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม (Digitalization: Digital ID - Overview)

(๒) แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย (Digitalization: Digital ID - Identity Proofing and Authentication)

(๓) แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับนิติบุคคล (Digitalization: Digital ID - Identity Proofing and Authentication)

(๔) แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติอื่น (Digitalization: Digital ID - Identity Proofing and Authentication)

(๕) แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการออกดิจิทัลไอดีสำหรับบริการภาครัฐ (Digitalization: Digital ID - Government Issued ID)

แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

๑. ที่มา เหตุผล และความจำเป็น

ตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ มาตรา ๑๒ (๒) กำหนดให้หน่วยงานของรัฐจัดทำกระบวนการหรือการดำเนินงานทางดิจิทัลเพื่อการบริหารราชการแผ่นดินและการให้บริการประชาชน กระบวนการหรือการดำเนินงานทางดิจิทัลนั้นต้องทำงานร่วมกันได้ตามมาตรฐาน ข้อกำหนด และหลักเกณฑ์ที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด เพื่อให้มีความสอดคล้องและเชื่อมโยงระหว่างหน่วยงานของรัฐแห่งอื่นได้ โดยมุ่งเน้นถึงการอำนวยความสะดวกและการเข้าถึงของประชาชนที่เป็นไปตามมาตรฐานและมีการบูรณาการข้อมูลระหว่างหน่วยงานของรัฐเป็นสำคัญ ประกอบมาตรา ๑๒ (๔) จัดให้มีระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อประโยชน์ในการอำนวยความสะดวกในการบริการประชาชน รวมถึงการให้บริการประชาชนที่ประสงค์จะลงทะเบียนและพิสูจน์ตัวตนผ่านระบบด้วยดิจิทัลไอดี (Digital Identity: Digital ID) ให้เป็นไปตามระดับความน่าเชื่อถือของไอเดนทิตี (Identity Assurance Level: IAL) และการยืนยันตัวตน (Authentication) ของผู้ใช้บริการที่ประสงค์จะใช้บริการภาครัฐผ่านระบบด้วยดิจิทัลไอดีที่เป็นไปตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level: AAL) ให้เป็นมาตรฐานเดียวกัน

ดังนั้นเพื่อให้หน่วยงานของรัฐสามารถดำเนินการเกี่ยวกับดิจิทัลไอดีตามที่ได้กล่าวข้างต้น จึงกำหนดแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

๒. ขอบข่าย

แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย ฉบับนี้เป็นข้อกำหนดและแนวทางในการพิสูจน์และยืนยันตัวตนทางดิจิทัลของผู้ใช้บริการที่ต้องการใช้บริการภาครัฐด้วยดิจิทัลไอดี เพื่อให้หน่วยงานที่เกี่ยวข้องกับการใช้ดิจิทัลไอดีมีความเข้าใจตรงกัน โดยอ้างอิงข้อกำหนด ดังนี้

๒.๑ มาตรฐาน NIST Special Publication 800-63-3 - Digital Identity Guidelines [๑]

๒.๒ มาตรฐาน NIST Special Publication 800-63A – Digital Identity Guidelines - Enrollment and Identity Proofing [๒]

๒.๓ มาตรฐาน NIST Special Publication 800-63B – Digital Identity Guidelines – Authentication and Lifecycle Management [๓]

๒.๔ ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ [๔]

๒.๕ ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน [๕]

๒.๖ ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน [๖]

๒.๗ ประกาศธนาคารแห่งประเทศไทย ที่ สนส. ๑๙/๒๕๖๒ เรื่อง หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน [๑๐]

๒.๘ ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทำธุรกรรมแบบพบเห็นลูกค้าต่อหน้าสำหรับธนาคาร [๑๑]

ในแนวทางฯ ฉบับนี้ รูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (Normative) และเนื้อหาเชิงให้ข้อมูล (Informative) [๑] มีดังนี้

– “ต้อง” (SHALL) ใช้ระบุสิ่งที่เป็นข้อกำหนด (Requirement) ที่ต้องปฏิบัติตาม

– “ควร” (SHOULD) ใช้ระบุสิ่งที่เป็นข้อแนะนำ (Recommendation)

– “อาจ” (MAY) ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้ (Permission)

๓. การทำความรู้จักผู้ใช้บริการ (Know Your Customer)

การทำความรู้จักผู้ใช้บริการ เป็นกระบวนการที่ผู้พิสูจน์และยืนยันตัวตนทำความรู้จักและพิสูจน์ตัวตนผู้ใช้บริการที่มาขอใช้บริการว่าเป็นบุคคลรายนั้นจริง เพื่อป้องกันการทุจริตจากการปลอมแปลงหรือใช้ข้อมูลของบุคคลอื่นในการใช้บริการภาครัฐ

กระบวนการทำความรู้จักผู้ใช้บริการ ประกอบด้วย ๒ ขั้นตอนที่สำคัญ ได้แก่ (๑) การแสดงตนเพื่อระบุตัวตน (Identification) และ (๒) การพิสูจน์ตัวตน (Identity Proofing) โดยมีข้อกำหนดที่ผู้พิสูจน์และยืนยันตัวตนต้องดำเนินการ [๑๐][๑๑] ดังนี้

๓.๑ ข้อกำหนดทั่วไป (General Requirements)

(๑) ต้องจัดให้ผู้ใช้บริการแสดงตนและตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบันของข้อมูลและเอกสารหลักฐานการแสดงตนที่ได้รับจากผู้ใช้บริการ รวมถึงตรวจสอบว่าบุคคลที่มาสมัครใช้บริการภาครัฐเป็นบุคคลเดียวกันกับบุคคลในหลักฐานแสดงตน

(๒) ต้องบริหารความเสี่ยงให้เหมาะสมและสอดคล้องกับความเสี่ยงของบริการภาครัฐ โดยกระบวนการทำความรู้จักผู้ใช้บริการแบบไม่พบเห็นต่อหน้าและแบบเสมือนพบเห็นต่อหน้าอาจมีความเสี่ยงสูงกว่าแบบพบเห็นต่อหน้า จึงต้องพิสูจน์ตัวตนในระดับที่เข้มข้นกว่า รวมถึงจัดให้มีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อบริหารความเสี่ยงให้มีประสิทธิภาพมากขึ้น

(๓) ต้องกำหนดนโยบายและกระบวนการปฏิบัติงานภายในที่ชัดเจนเป็นลายลักษณ์อักษร โดยต้องทบทวน สื่อสาร ทำความเข้าใจ สร้างความตระหนักให้กับเจ้าพนักงานหรือบุคลากรที่เกี่ยวข้องให้เห็นถึงความสำคัญ และปฏิบัติตามนโยบายและกระบวนการปฏิบัติงานภายในของผู้พิสูจน์และยืนยันตัวตนหรือหน่วยงานกำกับดูแลที่เกี่ยวข้อง นอกจากนี้ ต้องสื่อสารทำความเข้าใจและให้ความรู้กับผู้ใช้บริการด้วย

๓.๒ ข้อกำหนดการแสดงตนเพื่อระบุตัวตน (Identification Requirements)

ต้องได้รับข้อมูลและเอกสารหลักฐานการแสดงตนที่บ่งชี้ถึงตัวผู้สมัครใช้บริการ ซึ่งข้อมูลและเอกสารหลักฐานการแสดงตนดังกล่าวให้หมายรวมถึงข้อมูลและเอกสารอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย โดยต้องดำเนินการ ดังนี้

(๑) ข้อกำหนดของการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า กรณีระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๓ (IAL3)

(ก) ต้องมีเจ้าพนักงานที่มีอำนาจหน้าที่รับผิดชอบและผ่านการฝึกอบรมทำหน้าที่สังเกตสิ่งผิดปกติบนร่างกายของผู้สมัครใช้บริการ (เช่น ใบหน้า นิ้วมือ) และดำเนินการตรวจสอบตามกระบวนการพิสูจน์ตัวตน

(ข) ต้องรวบรวมข้อมูลชีวมิติในลักษณะที่มั่นใจว่าข้อมูลชีวมิติดังกล่าวถูกรวบรวมจากผู้สมัครใช้บริการ และไม่ใช่จากบุคคลอื่น

(๒) ข้อกำหนดของการพิสูจน์ตัวตนแบบเสมือนพบเห็นต่อหน้า กรณีระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๓ (IAL3)

(ก) ต้องเฝ้าสังเกตผู้สมัครใช้บริการตลอดเวลาของการพิสูจน์ตัวตน โดยที่ผู้สมัครใช้บริการต้องไม่ออกไปจากการสื่อสาร เช่น การเฝ้าสังเกตผู้สมัครใช้บริการด้วยการส่งผ่านวิดีโอที่มีความละเอียดสูงอย่างต่อเนื่อง (High Resolution Video Transmission)

(ข) ต้องมีเจ้าพนักงานที่มีอำนาจหน้าที่รับผิดชอบและผ่านการฝึกอบรม ทำหน้าที่เฝ้าสังเกตและเข้าร่วมสนทนาออนไลน์กับผู้สมัครใช้บริการแบบถ่ายทอดสดตลอดเวลาของการลงทะเบียนและพิสูจน์ตัวตน เช่น การส่งผ่านวิดีโอที่มีความละเอียดสูงอย่างต่อเนื่อง

(ค) เจ้าพนักงานต้องสามารถมองเห็นพฤติกรรมทั้งหมดของผู้สมัครใช้บริการระหว่างช่วงเวลาของการพิสูจน์ตัวตนได้อย่างชัดเจน

(ง) ต้องตรวจสอบหลักฐานแสดงตนด้วยวิธีการทางอิเล็กทรอนิกส์ โดยใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์หรือวิธีการที่เทียบเท่า เช่น การตรวจสอบลายมือชื่อที่ออกเอกสารแสดงตนในรูปแบบอิเล็กทรอนิกส์ และใช้เครื่องมืออุปกรณ์ของผู้พิสูจน์และยืนยันตัวตนทั้งหมด

(จ) ต้องฝึกอบรมเจ้าพนักงานเพื่อให้สามารถตรวจหาความผิดปกติที่อาจเกิดขึ้นในการพิสูจน์ตัวตนและดำเนินการได้อย่างเหมาะสม

(ฉ) ต้องติดตั้งระบบตรวจจับการบุกรุกทางกายภาพที่เหมาะสมกับสภาพแวดล้อมของสถานที่ตั้ง เช่น เครื่องให้บริการอัตโนมัติ (Kiosk) ที่ตั้งอยู่ในพื้นที่ที่จำกัดหรือพื้นที่ที่มีการรักษาความมั่นคงปลอดภัย

(ช) ต้องตรวจสอบให้มั่นใจว่าการติดต่อสื่อสารทั้งหมดเกิดขึ้นผ่านช่องทางการสื่อสารเฉพาะที่มีการป้องกัน

ทั้งนี้ รายละเอียดเพิ่มเติมของระดับความน่าเชื่อถือของไอเดนทิตี เป็นไปตามข้อ ๔.๑

๓.๓ ข้อกำหนดการพิสูจน์ตัวตน (Identity Proofing Requirements)

ต้องนำข้อมูลและเอกสารหลักฐานการแสดงตนมาตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบัน รวมถึงตรวจสอบตัวบุคคลว่าเป็นผู้สมัครใช้บริการรายนั้นจริง โดยต้องดำเนินการ ดังนี้

๓.๓.๑ การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า

(๑) ต้องตรวจสอบหลักฐานแสดงตนว่ามีความถูกต้อง ความแท้จริง และยังมีสถานะใช้งานได้

(๒) กรณีผู้สมัครใช้บริการแสดงบัตรประจำตัวประชาชน ต้องตรวจสอบสถานะของข้อมูลและบัตรประจำตัวประชาชนของผู้สมัครใช้บริการที่เป็นปัจจุบันผ่านระบบให้บริการของแหล่งให้ข้อมูลที่น่าเชื่อถือเพื่อทราบสถานะของข้อมูลและบัตรประจำตัวประชาชน

(๓) กรณีผู้สมัครใช้บริการแสดงเอกสารแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ต้องตรวจสอบความถูกต้อง ความแท้จริงของข้อมูล และเอกสารแสดงตนด้วยเครื่องมืออิเล็กทรอนิกส์ เพื่อป้องกันการปลอมแปลงข้อมูลบนหน้าเอกสารแสดงตน ทั้งนี้ หากผู้สมัครใช้บริการไม่มีเอกสารแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ หรือ

มีเหตุจำเป็นที่เอกสารแสดงตนที่มีข้อมูลอิเล็กทรอนิกส์บกพร่อง ให้บริหารความเสี่ยงที่เกี่ยวข้องอย่างเหมาะสมและรัดกุม

(๔) กรณีผู้สมัครใช้บริการให้ช่องทางการติดต่อเป็นหมายเลขโทรศัพท์หรืออีเมล ต้องตรวจสอบหมายเลขโทรศัพท์หรืออีเมลดังกล่าวของผู้สมัครใช้บริการว่าสามารถติดต่อได้จริง

(๕) กรณีเลือกใช้วิธีการตรวจสอบลักษณะที่ปรากฏเทียบกับรูปถ่ายจากหลักฐานแสดงตน (Physical Comparison) ต้องตรวจสอบว่าตรงกับลักษณะที่ปรากฏของผู้สมัครใช้บริการ เพื่อยืนยันว่าเป็นเจ้าของหลักฐานแสดงตนดังกล่าวจริง ทั้งนี้ กรณีผู้สมัครใช้บริการแสดงหลักฐานแสดงตนที่มีข้อมูลอิเล็กทรอนิกส์ ควรใช้รูปถ่ายที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์จากหลักฐานแสดงตนดังกล่าว เพื่อป้องกันการปลอมแปลงรูปถ่ายบนหน้าหลักฐานแสดงตน

(๖) กรณีเลือกใช้วิธีการตรวจสอบข้อมูลชีวมิติ (Biometric Comparison) เช่น ภาพใบหน้าหรือลายนิ้วมือ ต้องตรวจสอบเทียบกับข้อมูลชีวมิติจากหลักฐานแสดงตนว่าตรงกับผู้สมัครใช้บริการรายนั้นจริง

๓.๓.๒ การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า

(๑) ต้องตรวจสอบหลักฐานแสดงตนว่ามีความถูกต้อง ความแท้จริง และยังมีสถานะใช้งานได้

(๒) ต้องจัดให้มีกระบวนการลงทะเบียนและพิสูจน์ตัวตนผ่านระบบที่มีความน่าเชื่อถือและมีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยในการตรวจสอบข้อมูลและหลักฐานของผู้สมัครใช้บริการเทียบเท่ากับการพิสูจน์ตัวตนแบบพบเห็นต่อหน้าหรือเสมือนพบเห็นต่อหน้า

(๓) กรณีเลือกใช้วิธีการตรวจสอบลักษณะที่ปรากฏจากรูปถ่ายของผู้สมัครใช้บริการเทียบกับรูปถ่ายจากหลักฐานแสดงตน ต้องตรวจสอบว่าตรงกับลักษณะที่ปรากฏของผู้ใช้บริการเพื่อยืนยันว่าเป็นเจ้าของหลักฐานแสดงตนดังกล่าวจริง

(๔) กรณีเลือกใช้วิธีการตรวจสอบข้อมูลชีวมิติ เช่น ภาพใบหน้า หรือลายนิ้วมือ อาจใช้เทคโนโลยีเพื่อพิสูจน์ความเป็นบุคคลและสังเกตพฤติกรรมผู้สมัครใช้บริการ (Liveness Detection) และเทคโนโลยีเปรียบเทียบข้อมูลชีวมิติของผู้สมัครใช้บริการ เพื่อพิสูจน์ว่าเป็นผู้สมัครใช้บริการรายนั้นจริงทดแทนการพบเห็นต่อหน้า ถ้าไม่สามารถสังเกตพฤติกรรมของผู้สมัครใช้บริการ ต้องกำหนดกระบวนการหรือแนวทางการบริหารความเสี่ยงเพิ่มเติมเพื่อลดความเสี่ยงจากกรณีทุจริตต่าง ๆ ได้

๓.๓.๓ การพิสูจน์ตัวตนแบบเสมือนพบเห็นต่อหน้า

(๑) ต้องตรวจสอบหลักฐานแสดงตนว่ามีความถูกต้อง ความแท้จริง และยังมีสถานะใช้งานได้

(๒) ต้องจัดให้มีกระบวนการลงทะเบียนและพิสูจน์ตัวตนผ่านระบบที่มีความน่าเชื่อถือและมีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยในการตรวจสอบข้อมูลและหลักฐานของผู้สมัครใช้บริการเทียบเท่ากับการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า

(๓) ต้องจัดให้มีเจ้าพนักงานที่มีอำนาจหน้าที่รับผิดชอบและผ่านการฝึกอบรม ทำหน้าที่เฝ้าสังเกตและเข้าร่วมสนทนาออนไลน์กับผู้สมัครใช้บริการแบบถ่ายทอดสดตลอดเวลาของการลงทะเบียนและพิสูจน์ตัวตน

๔. ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล (Enrolment and Identity Proofing Requirements)

การลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลต้องทำให้มั่นใจได้ว่าผู้สมัครใช้บริการเป็นบุคคลที่กล่าวอ้างจริง โดยผ่านการแสดงตน (Presentation) การตรวจสอบหลักฐานแสดงตน (Validation) และการตรวจสอบตัวบุคคล (Verification) โดยผู้พิสูจน์และยืนยันตัวตนควรพิจารณาถึงความสมดุลระหว่างความเป็นส่วนบุคคลและความต้องการที่จะใช้ข้อมูลของผู้ใช้บริการ เพื่อกำหนดเป็นคุณลักษณะขั้นต่ำที่จำเป็น (Attribute) ในการพิสูจน์ตัวตนทางดิจิทัล เช่น เลขประจำตัวประชาชน ชื่อ ชื่อสกุล วันเดือนปีเกิด เลขหลังบัตรประจำตัวประชาชน (Laser Code)

๔.๑ ระดับความน่าเชื่อถือของไอเดนทิตี (Identity Assurance Level: IAL)

ระดับความน่าเชื่อถือของไอเดนทิตี คือ ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของผู้สมัครใช้บริการ การกำหนดระดับความน่าเชื่อถือของไอเดนทิตีที่เหมาะสมจะช่วยลดโอกาสของการพิสูจน์ตัวตนผิดพลาด โดยระดับความน่าเชื่อถือของไอเดนทิตี แบ่งออกเป็น ๓ ระดับ ดังนี้

(๑) ระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๑ (IAL1)

มีการรวบรวมข้อมูลเพื่อระบุตัวตน พิจารณาและตรวจสอบหลักฐานแสดงตนหรือไม่ก็ได้ ทั้งนี้ไม่มีข้อกำหนดในการแสดงตนและตรวจสอบตัวบุคคลโดยผู้พิสูจน์และยืนยันตัวตน เหมาะสำหรับบริการภาครัฐที่ไม่มีความเสี่ยงต่ำ

(๒) ระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๒ (IAL2)

กำหนดให้มีการรวบรวมข้อมูลเพื่อระบุตัวตน พิจารณาหลักฐานแสดงตน โดยผู้พิสูจน์และยืนยันตัวตนต้องตรวจสอบกับแหล่งให้ข้อมูลที่น่าเชื่อถือว่าไอเดนทิตีที่กล่าวอ้างมีอยู่ในโลกแห่งความจริง รวมถึงตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างการพิสูจน์ตัวตนที่ระดับ IAL2 สามารถทำได้ทั้งแบบพบเห็นต่อหน้า หรือ แบบไม่พบเห็นต่อหน้า

ทั้งนี้ ผู้พิสูจน์และยืนยันตัวตนที่รองรับระดับ IAL2 สามารถส่งผลการยืนยันตัวตนให้กับผู้ให้บริการภาครัฐที่ให้บริการที่ต้องการระดับ IAL1 ได้ หากผู้ใช้บริการให้ความยินยอม เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงปานกลางถึงความเสี่ยงสูง

(๓) ระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๓ (IAL3)

เพิ่มความเข้มงวดให้กับข้อกำหนดที่ระดับ IAL2 ด้วยการพิจารณาหลักฐานแสดงตนเพิ่มเติมและการตรวจสอบข้อมูลชีวมิติ เพื่อป้องกันการปลอมตัวเป็นบุคคลอื่น การหลอกลวงการลงทะเบียนซ้ำ หรือความเสียหายอื่น ๆ การพิสูจน์ตัวตนที่ระดับ IAL3 สามารถทำได้เฉพาะแบบพบเห็นต่อหน้า ซึ่งรวมถึงแบบเสมือนพบเห็นต่อหน้า

ทั้งนี้ ผู้พิสูจน์และยืนยันตัวตนที่รองรับระดับ IAL3 สามารถส่งผลการยืนยันตัวตนให้กับผู้ให้บริการภาครัฐที่ให้บริการที่ต้องการระดับ IAL1 และ IAL2 ได้ หากผู้ใช้บริการให้ความยินยอม เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงสูง

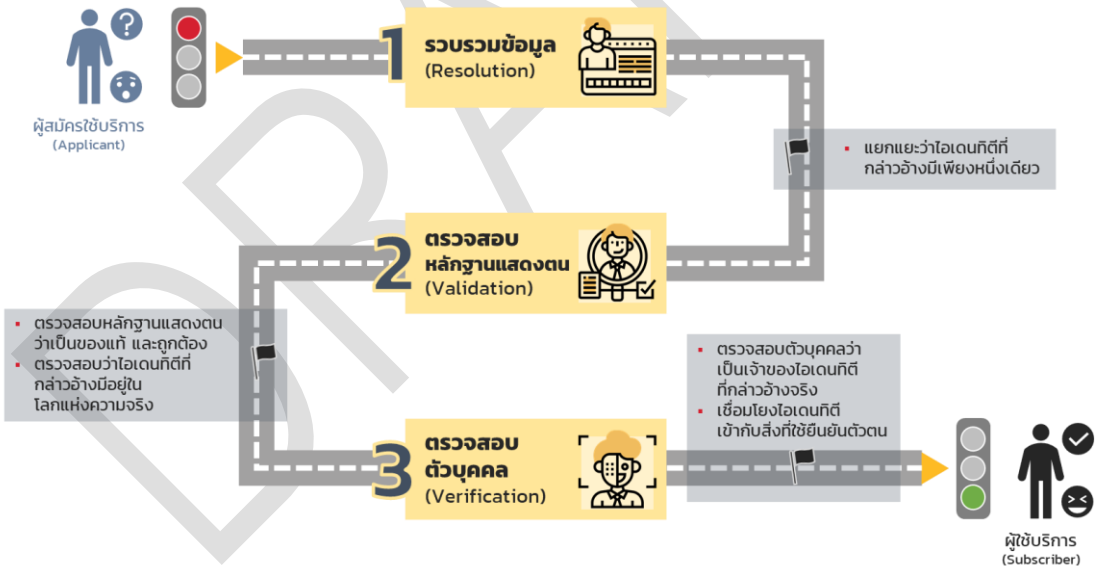
๔.๒ ขั้นตอนการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล (Process Flow)

เพื่อให้ขั้นตอนการรวบรวมและตรวจสอบข้อมูลหลักฐานของผู้สมัครใช้บริการ มีคุณภาพเพียงพอที่จะให้มั่นใจว่า (๑) ผู้สมัครใช้บริการมีตัวตนจริงและมีเพียงคนเดียว (๒) หลักฐานเป็นของแท้ มีข้อมูลถูกต้อง และ (๓) ผู้สมัครใช้บริการเป็นเจ้าของหลักฐานที่นำมาแสดง มีกระบวนการดำเนินการ ดังนี้

(๑) การรวบรวมข้อมูลเพื่อระบุตัวตน เป็นกระบวนการที่ผู้พิสูจน์และยืนยันตัวตนรวบรวมคุณลักษณะและหลักฐานแสดงตนที่จำเป็นจากผู้สมัครใช้บริการ เพื่อแยกแยะว่าไอเดนทิตีของผู้สมัครใช้บริการมีเพียงหนึ่งเดียวและมีความเฉพาะเจาะจงภายในบริบทของผู้ใช้บริการทั้งหมดที่ผู้พิสูจน์และยืนยันตัวตนดูแล ทั้งนี้ การระบุตัวตนที่ดีควรใช้ชุดของคุณลักษณะเท่าที่จำเป็นในการแยกแยะไอเดนทิตีของผู้สมัครใช้บริการแต่ละราย

(๒) การตรวจสอบหลักฐานแสดงตน เป็นกระบวนการที่ผู้พิสูจน์และยืนยันตัวตนตรวจสอบความแท้จริง สถานะการใช้งาน และความถูกต้องของหลักฐานแสดงตน รวมถึงตรวจสอบข้อมูลที่อยู่ในหลักฐานแสดงตนว่าเป็นของบุคคลที่มีตัวตนอยู่จริง

(๓) การตรวจสอบตัวบุคคล เป็นกระบวนการที่ผู้พิสูจน์และยืนยันตัวตนตรวจสอบตัวบุคคลที่แสดงหลักฐานแสดงตน ว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างจริง โดยอาจมีการตรวจสอบช่องทางติดต่อของผู้สมัครใช้บริการที่ได้ให้ไว้ในขั้นตอนการลงทะเบียนว่าเป็นเจ้าของช่องทางที่ใช้ในการติดต่อจริง รวมถึงสามารถติดต่อหรือส่งข้อมูลข่าวสารสำคัญไปยังผู้สมัครใช้บริการผ่านช่องทางดังกล่าวได้จริง



รูปที่ ๑ ขั้นตอนการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล

ที่มา: ปรับปรุงจาก (NIST, NIST Special Publication 800-63A – Digital Identity Guidelines - Enrollment and Identity Proofing, 2017) [๒]

จากรูปที่ ๑ แสดงให้เห็นขั้นตอนการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล มีทั้งหมด ๓ ขั้นตอน ได้แก่

(๑) รวบรวมข้อมูลเพื่อระบุตัวตน (Resolution)

การรวบรวมข้อมูลเพื่อระบุตัวตนมีจุดมุ่งหมายเพื่อแยกแยะว่าไอเดนทิตีที่กล่าวอ้างมีเพียงหนึ่งเดียว โดยใช้ชุดของคุณลักษณะที่ใช้ระบุตัวตนให้น้อยที่สุดเท่าที่จำเป็นเพื่อแยกแยะไอเดนทิตีที่กล่าวอ้างออกจาก

ไอเดนทิตีอื่น ซึ่งการรวบรวมข้อมูลเพื่อระบุตัวตนถือเป็นจุดเริ่มต้นของกระบวนการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล เช่น

- รวบรวมข้อมูลส่วนบุคคลจากผู้สมัครใช้บริการ เช่น เลขประจำตัวประชาชน ชื่อ ชื่อสกุล วันเดือนปีเกิด เลขหลังบัตรประจำตัวประชาชน อีเมล หมายเลขโทรศัพท์
- รวบรวมหลักฐานแสดงตน เช่น บัตรประจำตัวประชาชนหรือหนังสือเดินทาง โดยอาจมีการทำสำเนาหรือถ่ายภาพไว้เป็นหลักฐาน

(๒) ตรวจสอบหลักฐานแสดงตน (Validation)

การตรวจสอบหลักฐานแสดงตนมีจุดมุ่งหมายเพื่อรวบรวมหลักฐานการระบุตัวตนที่เหมาะสมที่สุดจากผู้สมัครใช้บริการเพื่อแสดงถึงความเป็นของแท้ สมบูรณ์ และถูกต้อง ซึ่งขั้นตอนของการตรวจสอบหลักฐานแสดงตน ประกอบด้วย การรวบรวมหลักฐานแสดงตนที่เหมาะสม การยืนยันหลักฐานแสดงตนว่าเป็นของแท้ และการยืนยันข้อมูลของหลักฐานแสดงตนว่าถูกต้อง เป็นปัจจุบัน และไอเดนทิตีที่กล่าวอ้างมีอยู่ในโลกแห่งความจริง เช่น

- ตรวจสอบข้อมูลที่ได้จากการรวบรวมข้อมูลตามข้อ (๑) กับแหล่งให้ข้อมูลที่น่าเชื่อถือโดยผู้พิสูจน์และยืนยันตัวตนต้องประเมินข้อมูลที่ได้รับจากผู้สมัครใช้บริการว่าตรงกัน
- ตรวจสอบสำเนาหรือภาพถ่ายของหลักฐานแสดงตนว่าไม่มีการปลอมแปลงแก้ไข เช่น เลขประจำตัวประชาชนที่อยู่ในสำเนาหรือภาพถ่ายต้องอยู่ในรูปแบบมาตรฐานที่กรมการปกครองกำหนด
- ตรวจสอบข้อมูลกับแหล่งออกหลักฐานแสดงตนว่าตรงกัน

(๓) ตรวจสอบตัวบุคคล (Verification)

การตรวจสอบตัวบุคคลมีจุดมุ่งหมายเพื่อยืนยันและเชื่อมโยงระหว่างไอเดนทิตีที่กล่าวอ้างกับบุคคลที่ยื่นหลักฐานแสดงตนว่าตรงกันและมีตัวตนอยู่ในโลกแห่งความจริง เช่น

- ให้ผู้สมัครใช้บริการถ่ายภาพตนเอง เพื่อพิสูจน์ความเป็นบุคคลและสังเกตพฤติกรรม (Liveness Check) และตรวจสอบกับหลักฐานแสดงตนว่าตรงกัน
- นำภาพถ่ายจากหลักฐานแสดงตนเทียบกับภาพถ่ายของผู้สมัครใช้บริการว่าตรงกัน
- อาจมีการส่งรหัสการลงทะเบียนไปยังหมายเลขโทรศัพท์ของผู้สมัครใช้บริการ โดยให้ผู้สมัครใช้บริการยืนยันรหัสการลงทะเบียนกลับมายังผู้พิสูจน์และยืนยันตัวตน โดยผู้พิสูจน์และยืนยันตัวตนเป็นผู้ยืนยันว่ารหัสดังกล่าวตรงกัน เพื่อเป็นการตรวจสอบว่าหมายเลขโทรศัพท์นั้นเป็นของผู้สมัครใช้บริการจริง

๔.๓ ข้อกำหนดทั่วไป (General Requirements)

ข้อกำหนดทั่วไปสำหรับผู้พิสูจน์และยืนยันตัวตนดำเนินการพิสูจน์ตัวตนที่ระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๒ หรือ ๓

(๑) การพิสูจน์ตัวตน<u>ต้องไม่</u>เป็นการประเมินถึงความเหมาะสม หรือการกำหนดสิทธิในการเข้าถึงบริการหรือสิทธิประโยชน์ต่าง ๆ

(๒) การรวบรวมข้อมูลส่วนบุคคล<u>ต้อง</u>รวบรวมให้น้อยที่สุดเท่าที่จำเป็นเพื่อตรวจสอบไอเดนทิตีที่กล่าวอ้างและเชื่อมโยงกับหลักฐานแสดงตนของผู้สมัครใช้บริการได้อย่างเหมาะสมสำหรับการ

รวบรวมข้อมูลเพื่อระบุตัวตน การตรวจสอบหลักฐานแสดงตน และการตรวจสอบตัวบุคคล ซึ่งอาจตรวจสอบหลักฐานแสดงตนกับแหล่งให้ข้อมูลที่น่าเชื่อถือและส่งให้ผู้ให้บริการภาครัฐใช้ในการตัดสินใจให้สิทธิเข้าใช้บริการ

(๓) ต้องแจ้งวัตถุประสงค์อย่างชัดเจนของการรวบรวมและจัดเก็บรักษาข้อมูลส่วนบุคคลที่ใช้สำหรับการพิสูจน์ตัวตนเท่าที่จำเป็น รวมถึงระบุคุณลักษณะที่ขึ้นอยู่กับความสมัครใจหรือคุณลักษณะที่จำเป็นต่อกระบวนการพิสูจน์ตัวตน และผลที่ตามมาหากผู้สมัครใช้บริการไม่แสดงคุณลักษณะดังกล่าว

(๔) ต้องไม่นำคุณลักษณะที่รวบรวมและจัดเก็บในกระบวนการพิสูจน์ตัวตนไปใช้กับวัตถุประสงค์อื่นนอกเหนือจากการพิสูจน์ตัวตน การยืนยันตัวตน หรือปฏิบัติตามที่กฎหมายกำหนด โดยผู้พิสูจน์และยืนยันตัวตนต้องมีมาตรการในการรับมือกับความเสี่ยงที่อาจเกิดขึ้นกับความเป็นส่วนบุคคล เพื่อป้องกันไม่ให้เกิดการทำผิดกฎหมาย เว้นแต่ผู้พิสูจน์และยืนยันตัวตนได้แจ้งให้ผู้สมัครใช้บริการทราบอย่างชัดเจน และได้รับความยินยอมให้นำคุณลักษณะไปใช้กับวัตถุประสงค์อื่น ๆ ทั้งนี้ผู้พิสูจน์และยืนยันตัวตนต้องไม่กำหนดการให้ความยินยอมให้นำคุณลักษณะไปใช้กับวัตถุประสงค์อื่น ๆ เป็นเงื่อนไขในการให้บริการ

(๕) ต้องจัดให้มีกลไกสำหรับการแก้ไขข้อร้องเรียนหรือปัญหาของผู้สมัครใช้บริการที่เกิดขึ้นจากการพิสูจน์ตัวตน โดยกลไกดังกล่าวต้องให้ผู้สมัครใช้บริการค้นหาและใช้งานได้ง่าย ทั้งนี้ผู้พิสูจน์และยืนยันตัวตนต้องประเมินประสิทธิภาพของกลไกต่าง ๆ ในการแก้ไขข้อร้องเรียนหรือปัญหาต่าง ๆ ที่เกิดขึ้น

(๖) ต้องดำเนินการตามนโยบายหรือแนวปฏิบัติของการลงทะเบียนและพิสูจน์ตัวตน ซึ่งระบุขั้นตอนของการตรวจสอบไอเดนทิตี โดยแนวปฏิบัติดังกล่าวต้องประกอบด้วยมาตรการควบคุมของผู้พิสูจน์และยืนยันตัวตนที่ต้องดำเนินการอย่างไร หากมีข้อผิดพลาดในการพิสูจน์ตัวตนที่ทำให้ผู้สมัครใช้บริการลงทะเบียนไม่สำเร็จ เช่น จำนวนครั้งที่อนุญาตให้ลองลงทะเบียนใหม่ ทางเลือกของการพิสูจน์ตัวตน (เช่น ระบบออนไลน์ล้มเหลว) หรือมาตรการรับมือการฉ้อโกงเมื่อตรวจพบความผิดปกติ

(๗) ต้องจัดเก็บบันทึก รวมถึงบันทึกการตรวจสอบ (Audit Log) ของรายละเอียดทุกขั้นตอนของการตรวจสอบไอเดนทิตีของผู้สมัครใช้บริการ และต้องบันทึกประเภทหลักฐานแสดงตนที่นำมาแสดงตนในขั้นตอนของการพิสูจน์ตัวตน ต้องดำเนินการตามกระบวนการบริหารจัดการความเสี่ยง รวมถึงการประเมินความเสี่ยงด้านความเป็นส่วนบุคคลและความมั่นคงปลอดภัยเพื่อกำหนด ดังนี้

(ก) ขั้นตอนเพิ่มเติมใด ๆ ที่ใช้ในการตรวจสอบไอเดนทิตีของผู้สมัครใช้บริการ นอกเหนือจากข้อกำหนดที่ต้องปฏิบัติตามซึ่งระบุไว้ในแนวทางฯ ฉบับนี้

(ข) ข้อมูลส่วนบุคคล รวมถึงข้อมูลชีวมิติ รูปภาพ ภาพสแกน หรือสำเนาของหลักฐานแสดงตนอื่น ๆ ที่ผู้พิสูจน์และยืนยันตัวตนต้องจัดเก็บไว้เป็นบันทึกของการพิสูจน์ตัวตน

(ค) ระยะเวลาของการจัดเก็บบันทึกของการพิสูจน์ตัวตนให้เป็นไปตามกฎหมาย กฎระเบียบหรือนโยบายต่าง ๆ ที่เกี่ยวข้อง

(๘) ข้อมูลส่วนบุคคลทั้งหมดที่ได้รวบรวมมาจากกระบวนการลงทะเบียน ต้องมีการปกป้องเพื่อให้มั่นใจได้ว่ามีการรักษาความลับ (Confidentiality) มีความครบถ้วน ถูกต้อง สมบูรณ์ (Integrity) และระบุแหล่งที่มาของข้อมูล (Attribution of the Information Source)

(๙) การทำธุรกรรมที่เกี่ยวกับการพิสูจน์ตัวตนทั้งหมด รวมถึงธุรกรรมที่เกี่ยวข้องกับบุคคลที่สาม ต้องดำเนินการผ่านช่องทางการติดต่อสื่อสารที่มีความมั่นคงปลอดภัย

(๑๐) ควรมีมาตรการเพิ่มเติมเพื่อบรรเทาการฉ้อโกงและเพิ่มความน่าเชื่อถือในการพิสูจน์ตัวตน เช่น การตรวจสอบตำแหน่งทางภูมิศาสตร์ การตรวจสอบอุปกรณ์ การตรวจสอบลักษณะและพฤติกรรมของผู้สมัครใช้บริการ และต้องประเมินความเสี่ยงด้านความเป็นส่วนบุคคลสำหรับมาตรการดังกล่าวข้างต้น ซึ่งการประเมินความเสี่ยงดังกล่าวต้องรวมถึงการบรรเทาความเสี่ยง เช่น การยอมรับหรือถ่ายโอนความเสี่ยง การจัดเก็บในระยะเวลาที่จำกัด การจำกัดการใช้ข้อมูล และการแจ้งข้อมูล รวมถึงการใช้เทคโนโลยีเพื่อช่วยบรรเทาความเสี่ยง เช่น การเข้ารหัส (Cryptography) และการจัดทำเอกสารตามข้อกำหนดที่ ๔.๓ (๗)

(๑๑) เมื่อกระบวนการลงทะเบียนและพิสูจน์ตัวตนสิ้นสุดลง ต้องกำจัดหรือทำลายข้อมูลที่มีความอ่อนไหว (Sensitive Data) รวมถึงข้อมูลส่วนบุคคล หรือการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตตลอดช่วงระยะเวลาของเก็บรักษาข้อมูล

๔.๔ ข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๑ (IAL1)

ผู้พิสูจน์และยืนยันตัวตนต้องดำเนินการตามข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๑ ดังนี้

(๑) รวบรวมข้อมูลส่วนบุคคลเพื่อระบุตัวตนของผู้สมัครใช้บริการหรือไม่ก็ได้

(๒) กรณีขอหลักฐานแสดงตนที่ยังไม่หมดอายุจากผู้สมัครใช้บริการ มีดังนี้

(ก) บัตรประจำตัวประชาชน **หรือ**

(ข) หนังสือเดินทาง **หรือ**

(ค) เอกสารแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ

(๓) ตรวจสอบข้อมูลหรือเอกสารหลักฐานที่นำมาเป็นหลักฐานแสดงตนตาม ๔.๔ (๒) ว่าเป็นของแท้และถูกต้อง

(๔) ตรวจสอบช่องทางการติดต่อว่าสามารถติดต่อผู้สมัครใช้บริการได้

๔.๕ ข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๒ (IAL2)

ผู้พิสูจน์และยืนยันตัวตนต้องดำเนินการตามข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๒ ดังนี้

(๑) ต้องรองรับการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า **หรือ** ไม่พบเห็นต่อหน้า ทั้งนี้ควรจัดให้มีการพิสูจน์ตัวตนทั้งสองรูปแบบสำหรับการแสดงตนของผู้สมัครใช้บริการ

(๒) การรวบรวมข้อมูลเพื่อระบุตัวตน

(ก) ต้องรวบรวมข้อมูลส่วนบุคคลของผู้สมัครใช้บริการเท่าที่จำเป็น เพื่อแยกแยะว่าไอเดนทิตีของผู้สมัครใช้บริการมีเพียงหนึ่งเดียวและมีความเฉพาะเจาะจงภายในบริบทของผู้ใช้บริการทั้งหมดที่ผู้พิสูจน์และยืนยันตัวตนดูแล ซึ่งอาจรวมถึงการรวบรวมคุณลักษณะเพื่อช่วยในการค้นหาข้อมูล

(ข) อาจใช้การยืนยันด้วยชุดข้อมูลที่รู้เฉพาะผู้สมัครใช้บริการ (Knowledge-based Verification: KBV)

(๓) ต้องขอหลักฐานแสดงตนที่ยังไม่หมดอายุจากผู้สมัครใช้บริการ ดังนี้

(ก) บัตรประจำตัวประชาชน **หรือ**

(ข) หนังสือเดินทาง **หรือ**

(ค) เอกสารแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ

(๔) การตรวจสอบหลักฐานแสดงตน

(ก) ต้องตรวจสอบหลักฐานแสดงตนตาม ๔.๕ (๓) โดยใช้เจ้าพนักงานหรือเทคโนโลยีที่เหมาะสมว่าเป็นของแท้

(ข) ต้องตรวจสอบข้อมูลของหลักฐานแสดงตนตาม ๔.๕ (๓) โดยเปรียบเทียบกับข้อมูลจากแหล่งให้ข้อมูลที่น่าเชื่อถือว่ามีความถูกต้อง

(๕) การตรวจสอบตัวบุคคล

(ก) ต้องตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง โดยเปรียบเทียบลักษณะที่ปรากฏของผู้สมัครใช้บริการกับรูปถ่ายจากหลักฐานแสดงตน **หรือ** เปรียบเทียบข้อมูลชีวมิติของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน

(ข) อาจบันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (Biometric Sample) (เช่น ภาพใบหน้า ลายนิ้วมือ) เพื่อวัตถุประสงค์ในการห้ามปฏิเสธความรับผิด (Non-repudiation) และการตรวจสอบอีกครั้งในกรณีจำเป็น (Re-proofing)

(๖) การตรวจสอบช่องทางการติดต่อ

(ก) ต้องตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถติดต่อได้จริง เช่น การตรวจสอบอีเมลด้วยวิธีการยืนยันทางอีเมล การตรวจสอบหมายเลขโทรศัพท์ด้วยรหัสผ่านแบบใช้ครั้งเดียว (OTP) หรือวิธีการยืนยันทาง SMS

๔.๖ ข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๓ (IAL3)

ผู้พิสูจน์และยืนยันตัวตนต้องดำเนินการตามข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตีระดับที่ ๓ ดังนี้

(๑) ต้องพิสูจน์ตัวตนแบบพบเห็นต่อหน้า **หรือ** เสมือนพบเห็นต่อหน้า ทั้งนี้ควรจัดให้มีการพิสูจน์ตัวตนทั้งสองรูปแบบสำหรับการแสดงตนเพื่อระบุตัวตนของผู้สมัครใช้บริการ โดยปฏิบัติตามข้อกำหนด ๓.๒

(๒) การรวบรวมข้อมูลเพื่อระบุตัวตน

(ก) ข้อกำหนดเช่นเดียวกับ IAL2

(๓) ต้องขอหลักฐานแสดงตนที่ยังไม่หมดอายุจากผู้สมัครใช้บริการ โดยมีทางเลือก ดังนี้

(ก) บัตรประจำตัวประชาชนและหนังสือเดินทาง **หรือ**

(ข) ใช้การตรวจสอบหลักฐานเอกสารแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ๒ ชิ้นขึ้นไป **หรือ**

(ค) บัตรประจำตัวประชาชนและแหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่น ๒ แหล่งขึ้นไป

(๔) การตรวจสอบหลักฐานแสดงตน

(ก) ข้อกำหนดเช่นเดียวกับ IAL2

(๕) การตรวจสอบตัวบุคคล

(ก) ต้องตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง โดยเปรียบเทียบข้อมูลชีวมิติของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน

(ข) ต้องบันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (เช่น ภาพใบหน้า ลายนิ้วมือ) เพื่อวัตถุประสงค์ในการห้ามปฏิเสธความรับผิด และการตรวจสอบอีกครั้งในกรณีจำเป็น

(๖) การตรวจสอบช่องทางการติดต่อ

(ก) ข้อกำหนดเช่นเดียวกับ IAL2

๔.๗ สรุปข้อกำหนดระดับความน่าเชื่อถือของไอเดนทิตี (Summary of Requirements)

ตารางที่ ๑ สรุปข้อกำหนดระดับความน่าเชื่อถือของไอเดนทิตี

ข้อกำหนด	IAL1	IAL2	IAL3
การแสดงตน	ไม่มีข้อกำหนด	ต้องรองรับการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า **หรือ** ไม่พบเห็นต่อหน้า	ต้องพิสูจน์ตัวตนแบบพบเห็นต่อหน้า **หรือ** เสมือนพบเห็นต่อหน้า
การรวบรวมข้อมูลเพื่อระบุตัวตน	รวบรวมข้อมูลเพื่อระบุตัวบุคคลหรือไม่ก็ได้	- ต้องรวบรวมข้อมูลเพื่อระบุตัวบุคคล - อาจใช้ชุดข้อมูลที่รู้เฉพาะผู้สมัครใช้บริการ (Knowledge-based verification : KBV)	เช่นเดียวกับ IAL2
การขอหลักฐานแสดงตน	ขอหลักฐานแสดงตนที่ยังไม่หมดอายุหรือไม่ก็ได้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - เอกสารแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ	ต้องขอหลักฐานแสดงตนที่ยังไม่หมดอายุ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - เอกสารแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ	ต้องขอหลักฐานแสดงตนที่ยังไม่หมดอายุ - ทางเลือกที่ ๑ บัตรประจำตัวประชาชน และ หนังสือเดินทาง **หรือ** - ทางเลือกที่ ๒ ตรวจสอบหลักฐานเอกสารแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ๒ ชิ้นขึ้นไป **หรือ** - ทางเลือกที่ ๓ บัตรประจำตัวประชาชน และ แหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่น ๒ แหล่งขึ้นไป
การตรวจสอบหลักฐานแสดงตน	ตรวจสอบและเปรียบเทียบหลักฐานแสดงตนที่ยังไม่หมดอายุว่าเป็นของแท้และถูกต้องหรือไม่ก็ได้	- ต้องตรวจสอบหลักฐานแสดงตน โดยใช้เจ้าพนักงานหรือเทคโนโลยีที่เหมาะสมว่าเป็นของแท้	เช่นเดียวกับ IAL2

ข้อกำหนด	IAL1	IAL2	IAL3
		- ต้องตรวจสอบข้อมูลของหลักฐานแสดงตน โดยเปรียบเทียบกับข้อมูลจากแหล่งให้ข้อมูลที่น่าเชื่อถือว่ามีความถูกต้อง	
การตรวจสอบตัวบุคคล	ไม่ตรวจสอบตัวบุคคล	ต้องตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง โดย - เปรียบเทียบลักษณะที่ปรากฏเทียบกับรูปถ่ายจากหลักฐานแสดงตน (Physical Comparison) **หรือ** - เปรียบเทียบภาพใบหน้า หรือลายนิ้วมือเทียบกับข้อมูลชีวมิติจากหลักฐานแสดงตน (Biometric Comparison)	ต้องตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง โดย - เปรียบเทียบภาพใบหน้า หรือลายนิ้วมือเทียบกับข้อมูลชีวมิติจากหลักฐานแสดงตน (Biometric Comparison)
การรวบรวมข้อมูลชีวมิติ	ไม่มีข้อกำหนด	บันทึกตัวอย่างข้อมูลชีวมิติ (Biometric Sample) หรือไม่ก็ได้	ต้องบันทึกตัวอย่างข้อมูลชีวมิติ (Biometric Sample)
การตรวจสอบช่องทางการติดต่อ	ตรวจสอบช่องทางว่าสามารถติดต่อได้ - หมายเลขโทรศัพท์ **หรือ** - อีเมล	ต้องตรวจสอบช่องทางการติดต่อ - หมายเลขโทรศัพท์ **หรือ** - อีเมล	เช่นเดียวกับ IAL2

๔.๘ ข้อกำหนดขั้นต่ำในการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล (Minimum Requirements for Enrolment and Identity Proofing)

ผู้พิสูจน์และยืนยันตัวตนระบุข้อกำหนดในการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลให้เป็นไปตามกลุ่มการให้บริการภาครัฐ ทั้ง ๔ กลุ่ม โดยต้องประเมินความต้องการของหน่วยงาน ความเสี่ยง และระดับความน่าเชื่อถือ โดยเลือกวิธีการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลที่เหมาะสม เพื่อให้ขั้นตอนการรวบรวม และตรวจสอบข้อมูลหลักฐานผู้สมัครใช้บริการ มีคุณภาพเพียงพอที่จะให้มั่นใจว่า (๑) ผู้สมัครใช้บริการมีตัวตนจริงและมีเพียงคนเดียว (๒) หลักฐานเป็นของแท้ มีข้อมูลถูกต้อง และ (๓) ผู้สมัครใช้บริการเป็นเจ้าของหลักฐานที่นำมาแสดง

ข้อกำหนดขั้นต่ำในการกำหนดระดับความน่าเชื่อถือของไอเดนทิตีในการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล จำแนกตามกลุ่มการให้บริการภาครัฐ ดังนี้

(๑) กลุ่มการให้บริการข้อมูลพื้นฐาน จัดเป็นบริการที่ไม่มีความเสี่ยงหรือความเสี่ยงต่ำ จึง**ไม่จำเป็นต้องใช้ดิจิทัลไอดี**

(๒) กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ จัดเป็นบริการที่มีความเสี่ยงต่ำ สามารถใช้การพิสูจน์ตัวตนในระดับความน่าเชื่อถือของไอเดนทิตี **อย่างน้อยระดับที่ ๑**

(๓) กลุ่มการให้บริการธุรกรรม จัดเป็นบริการที่มีความเสี่ยงปานกลางถึงสูง เนื่องจากการให้บริการดังกล่าว ผู้พิสูจน์และยืนยันตัวตนต้องตรวจสอบความถูกต้อง ความแท้จริงของผู้สมัครใช้บริการ โดยการตรวจสอบผ่านแหล่งให้ข้อมูลที่น่าเชื่อถือเพื่อให้มั่นใจว่าผู้สมัครใช้บริการเป็นบุคคลเดียวกับหลักฐานแสดงตนนั้นจริง จึงจะสามารถทำธุรกรรมทางอิเล็กทรอนิกส์ได้ สามารถใช้การพิสูจน์ตัวตนในระดับความน่าเชื่อถือของไอเดนทิตี **อย่างน้อยระดับที่ ๒**

(๔) กลุ่มให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงาน จัดเป็นบริการที่มีความเสี่ยงสูง และต้องรู้จักตัวตนของผู้ใช้บริการ สามารถใช้การพิสูจน์ตัวตนในระดับความน่าเชื่อถือของไอเดนทิตี **อย่างน้อยระดับที่ ๓**

หมายเหตุ กรณีที่ต้องมีการตรวจสอบหลักฐานแสดงตนกับแหล่งให้ข้อมูลที่น่าเชื่อถือมากกว่า ๑ แหล่งขึ้นไป ให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เช่น ศูนย์แลกเปลี่ยนข้อมูลกลาง โดยไม่ต้องร้องขอข้อมูลจากผู้สมัครใช้บริการเพิ่มเติม

รายละเอียดแนวทางการกำหนดระดับความน่าเชื่อถือของไอเดนทิตีของกลุ่มการให้บริการภาครัฐ ดังตารางที่ ๒

ตารางที่ ๒ แนวทางการกำหนดระดับความน่าเชื่อถือของไอเดนทิตีของกลุ่มการให้บริการภาครัฐ

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ	IAL1	การรวบรวมข้อมูลเพื่อระบุตัวตน	เจ้าพนักงานรวบรวมข้อมูลระบุตัวบุคคลของผู้สมัครใช้บริการหรือไม่ก็ได้	เจ้าพนักงานรวบรวมข้อมูลระบุตัวบุคคลของผู้สมัครใช้บริการผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนด เพื่อแสดงตนหรือไม่ก็ได้	เจ้าพนักงานรวบรวมข้อมูลระบุตัวบุคคลของผู้สมัครใช้บริการผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนด เพื่อแสดงตนหรือไม่ก็ได้
		การตรวจสอบหลักฐานแสดงตน	IdP ตรวจสอบข้อมูลหลักฐานแสดงตนยังไม่หมดอายุหรือไม่ก็ได้ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - เอกสารแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ	IdP ตรวจสอบข้อมูลหลักฐานแสดงตนยังไม่หมดอายุหรือไม่ก็ได้ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** หนังสือเดินทาง - ผู้สมัครใช้บริการถ่ายรูปหลักฐานแสดงตนผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดของ IdP และเจ้าพนักงานดูรูปหลักฐานแสดงตนเพื่อตรวจสอบว่าเป็นของแท้ - เจ้าพนักงานเปรียบเทียบข้อมูลของผู้สมัครใช้	IdP ตรวจสอบข้อมูลหลักฐานแสดงตนยังไม่หมดอายุหรือไม่ก็ได้ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** หนังสือเดินทาง - ผู้สมัครใช้บริการถ่ายรูปหลักฐานแสดงตนผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดของ IdP และเจ้าพนักงานดูรูปหลักฐานแสดงตนเพื่อตรวจสอบว่าเป็นของแท้ - เจ้าพนักงานเปรียบเทียบข้อมูลของผู้สมัครใช้

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
				บริการกับข้อมูลบนหลักฐานแสดงตน เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง	บริการกับข้อมูลบนหลักฐานแสดงตน เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง
		การตรวจสอบตัวบุคคล	ไม่มีข้อกำหนด	ไม่มีข้อกำหนด	ไม่มีข้อกำหนด
		การตรวจสอบช่องทางติดต่อ	IdP ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริงหรือไม่ก็ได้ เช่น อีเมล หมายเลขโทรศัพท์	IdP ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริงหรือไม่ก็ได้ เช่น อีเมล หมายเลขโทรศัพท์	IdP ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริงหรือไม่ก็ได้ เช่น อีเมล หมายเลขโทรศัพท์
กลุ่มการให้บริการธุรกรรม	IAL2	การรวบรวมข้อมูลเพื่อระบุตัวตน	ผู้สมัครใช้บริการ <u>ต้อง</u>ให้ข้อมูลเพื่อแสดงตน โดยเจ้าพนักงานรวบรวมข้อมูลระบุตัวบุคคล เช่น ชื่อ ชื่อสกุล ที่อยู่ อีเมล หมายเลขโทรศัพท์	ผู้สมัครใช้บริการ <u>ต้อง</u>ให้ข้อมูลผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดของ IdP โดยเจ้าพนักงานรวบรวมข้อมูลระบุตัวบุคคล	ผู้สมัครใช้บริการ <u>ต้อง</u>ให้ข้อมูลผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดของ IdP โดยเจ้าพนักงานรวบรวมข้อมูลระบุตัวบุคคล
		การตรวจสอบหลักฐานแสดงตน	IdP <u>ต้อง</u>ตรวจสอบข้อมูลหลักฐานแสดงตนที่ยังไม่หมดอายุ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ**	IdP <u>ต้อง</u>ตรวจสอบข้อมูลหลักฐานแสดงตนที่ยังไม่หมดอายุ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ**	IdP <u>ต้อง</u>ตรวจสอบข้อมูลหลักฐานแสดงตนที่ยังไม่หมดอายุ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ**

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
			- เอกสารแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ - เจ้าพนักงานใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์ เพื่อตรวจสอบหลักฐานแสดงตนว่าเป็นของแท้ - เจ้าพนักงานเปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง	- เอกสารแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ - ผู้สมัครใช้บริการใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์หรือเทคโนโลยีที่กำหนดของ IdP เพื่อตรวจสอบหลักฐานแสดงตนว่าเป็นของแท้ - IdP เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง	- เอกสารแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ - ผู้สมัครใช้บริการใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์หรือเทคโนโลยีที่กำหนดของ IdP เพื่อตรวจสอบหลักฐานแสดงตนว่าเป็นของแท้ - เจ้าพนักงานเปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง
		การตรวจสอบตัวบุคคล	- เจ้าพนักงานอาจถ่ายรูปและบันทึกภาพใบหน้าของผู้สมัครใช้บริการ เพื่อใช้เป็นหลักฐาน - เจ้าพนักงานเปรียบเทียบลักษณะที่ปรากฏของผู้สมัครใช้บริการกับรูป	- ผู้สมัครใช้บริการถ่ายรูปตัวเองพร้อมหลักฐานแสดงตนผ่านแอปพลิเคชันของ IdP และ IdP บันทึกภาพใบหน้าของผู้สมัครใช้บริการ เพื่อใช้เป็นหลักฐาน	- ผู้สมัครใช้บริการถ่ายรูปตัวเองผ่านแอปพลิเคชัน เว็บไซต์หรือเทคโนโลยีที่กำหนดของ IdP และ IdP บันทึกภาพใบหน้าของ

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
			ถ่ายจากหลักฐานแสดงตน (Physical Comparison) - กรณีใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (Biometric Comparison)	- เจ้าพนักงานเปรียบเทียบรูปถ่ายของผู้สมัครใช้บริการกับรูปถ่ายจากหลักฐานแสดงตน (Physical Comparison) - กรณีใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (Biometric Comparison)	ผู้สมัครใช้บริการเพื่อใช้เป็นหลักฐาน - เจ้าพนักงานเปรียบเทียบรูปถ่ายของผู้สมัครใช้บริการกับรูปถ่ายจากหลักฐานแสดงตน (Physical Comparison) - กรณีใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (Biometric Comparison)
		การตรวจสอบช่องทางติดต่อ	IdP ต้องตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง เช่น อีเมล หมายเลขโทรศัพท์	IdP ต้องตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง เช่น อีเมล หมายเลขโทรศัพท์	IdP ต้องตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง เช่น อีเมล หมายเลขโทรศัพท์

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงาน	IAL3	การรวบรวมข้อมูลเพื่อระบุตัวตน	ผู้สมัครใช้บริการต้องให้ข้อมูลเพื่อแสดงตนโดยเจ้าพนักงานรวบรวมข้อมูลระบุตัวบุคคล		ผู้สมัครใช้บริการต้องให้ข้อมูลผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดของ IdP โดยเจ้าพนักงานรวบรวมข้อมูลระบุตัวบุคคล
		การตรวจสอบหลักฐานแสดงตน	IdP ต้องขอหลักฐานแสดงตนที่ยังไม่หมดอายุ ดังนี้ - ทางเลือกที่ ๑ บัตรประจำตัวประชาชน และ หนังสือเดินทาง **หรือ** - ทางเลือกที่ ๒ ตรวจสอบหลักฐานเอกสารแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ๒ ชิ้น ขึ้นไป **หรือ** - ทางเลือกที่ ๓ บัตรประจำตัวประชาชน และ แหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่น ๒ แหล่งขึ้นไป		IdP ต้องขอหลักฐานแสดงตนที่ยังไม่หมดอายุ ดังนี้ - ทางเลือกที่ ๑ บัตรประจำตัวประชาชน และ หนังสือเดินทาง **หรือ** - ทางเลือกที่ ๒ ตรวจสอบหลักฐานเอกสารแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ๒ ชิ้น ขึ้นไป **หรือ** - ทางเลือกที่ ๓ บัตรประจำตัวประชาชน และ แหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่น ๒ แหล่งขึ้นไป

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
			- เจ้าพนักงานดูหลักฐานแสดงตน และใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์หรือตรวจสอบแหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่นเพื่อตรวจสอบว่าเป็นของแท้ - เจ้าพนักงานเปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง		- เจ้าพนักงานดูหลักฐานแสดงตน และใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์หรือตรวจสอบแหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่นเพื่อตรวจสอบว่าเป็นของแท้ - เจ้าพนักงานเปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง
		การตรวจสอบตัวบุคคล	- เจ้าพนักงานบันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (Biometric Sample) เช่น ภาพใบหน้า ลายนิ้วมือ		- เจ้าพนักงานบันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (Biometric Sample) เช่น ภาพใบหน้า ลายนิ้วมือ

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
			- ใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (Biometric Comparison)		- ใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (Biometric Comparison)
		การตรวจสอบช่องทางการติดต่อ	IdP ต้องตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง เช่น อีเมล หมายเลขโทรศัพท์		IdP ต้องตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง เช่น อีเมล หมายเลขโทรศัพท์

การยืนยันตัวตนทางดิจิทัล (Authentication)

๕. ข้อกำหนดการยืนยันตัวตนทางดิจิทัล (Authentication Requirements)

ข้อกำหนดของการยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐ ให้เป็นไปตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน [๖] ข้อ ๒. ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level) โดยปัจจัยของการยืนยันตัวตน (Authentication Factor) มีรายละเอียดตามแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม ข้อ ๕.๓.๑ สิ่งที่ใช้ยืนยันตัวตน (Authenticator)

๕.๑ ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level: AAL)

ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน คือ ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของผู้ใช้บริการ ซึ่งการกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนที่เหมาะสมจะช่วยลดโอกาสของการยืนยันตัวตนผิดพลาด แบ่งออกเป็น ๓ ระดับ ดังนี้

(๑) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ระดับที่ ๑ (AAL1)

กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบปัจจัยเดียว (Single-factor Authentication) เป็นอย่างน้อย หรือหากต้องการความมั่นคงปลอดภัยที่สูงขึ้น สามารถยืนยันตัวตนแบบหลายปัจจัยได้ (Multi-factor Authentication) และต้องเป็นโพรโทคอลที่มีความปลอดภัย (Secure Authentication Protocol) เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงต่ำ

(๒) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ระดับที่ ๒ (AAL2)

กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบ ๒ ปัจจัยที่แตกต่างกัน ซึ่งอาจเป็น (๑) สิ่งที่ใช้ยืนยันตัวตนหลายปัจจัย (Multi-factor Authenticator) เช่น อุปกรณ์ OTP แบบหลายปัจจัย (Multi-factor OTP Device) ซึ่งจะสร้างรหัสผ่านแบบใช้ครั้งเดียวหลังจากตรวจสอบลายนิ้วมือของผู้ใช้บริการ หรือ (๒) สิ่งที่ใช้ยืนยันตัวตนแบบปัจจัยเดียว (Single-factor Authenticator) อย่างน้อย ๒ สิ่งที่เป็นปัจจัยต่างกัน โดยที่ต้องเป็นรหัสลับจดจำ (Something You Know) และเป็นสิ่งที่ผู้ใช้บริการครอบครอง (Something You Have) เช่น การใช้รหัสผ่านควบคู่กับการใช้ OTP ผ่านหมายเลขโทรศัพท์ โดยโพรโทคอลที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตนต้องเป็นโพรโทคอลที่มีความปลอดภัย เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงปานกลางถึงความเสี่ยงสูง

(๓) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ระดับที่ ๓ (AAL3)

กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบ ๒ ปัจจัยขึ้นไปที่แตกต่างกัน โดยมีปัจจัยหนึ่งเป็นกุญแจ (Key) ที่ผ่านเกณฑ์วิธีการเข้ารหัสลับ (Cryptographic Protocol) ซึ่งผู้ใช้บริการต้องพิสูจน์ว่าตนครอบครองกุญแจนั้น และต้องพิสูจน์ว่าตนครอบครองปัจจัยของการยืนยันตัวตนดังกล่าว ผ่านโพรโทคอลที่มีความปลอดภัยในการใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน และต้องมีการเข้ารหัสข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหว รวมถึงสิ่งที่ใช้ยืนยันตัวตนเพื่อป้องกันการปลอมแปลง เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงสูง

๕.๒ ชนิดและข้อกำหนดสิ่งที่ใช้ยืนยันตัวตน (Authenticator and Verifier Requirements)

ข้อกำหนดของการยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐ ให้เป็นไปตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน [๖] ข้อ ๓. ชนิดและข้อกำหนดสิ่งที่ใช้ยืนยันตัวตน

ทั้งนี้ การเปลี่ยนแปลงทางเทคโนโลยีหรือภัยคุกคาม อาจเกิดข้อจำกัดของสิ่งที่ใช้ยืนยันตัวตนที่ทำให้เสื่อมคุณภาพลง (Restricted Authenticator) โดยผู้พิสูจน์และยืนยันตัวตนต้องดำเนินการ ดังนี้

(๑) เสนอทางเลือกของสิ่งที่ใช้ยืนยันตัวตนที่ยังไม่เสื่อมคุณภาพและสอดคล้องกับข้อกำหนดของระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

(๒) จัดทำเอกสารแจ้งข้อมูล (Notice) ให้ผู้ใช้บริการทราบถึงความเสี่ยงด้านความมั่นคงปลอดภัยของสิ่งที่ใช้ยืนยันตัวตนที่เสื่อมคุณภาพ รวมถึงทางเลือกของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้

(๓) ประเมินความเสี่ยงเกี่ยวกับสิ่งที่ใช้ยืนยันตัวตนที่อาจเสื่อมคุณภาพลงของผู้ใช้บริการเพิ่มเติม

(๔) จัดทำแผนการบรรเทาความเสี่ยงสิ่งที่ใช้ยืนยันตัวตนที่อาจเสื่อมคุณภาพ

๕.๓ การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน (Authenticator Lifecycle Management)

การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน ประกอบด้วยกระบวนการ ดังนี้

๕.๓.๑ การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน (Authenticator Binding)

การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน คือ การสร้างความสัมพันธ์ระหว่างสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตีของผู้ใช้บริการที่ออกโดยผู้พิสูจน์และยืนยันตัวตนในขั้นตอนของการลงทะเบียน เพื่อนำสิ่งที่ใช้ยืนยันตัวตนไปใช้ในการยืนยันตัวตนของผู้ใช้บริการ

โดยผู้พิสูจน์และยืนยันตัวตน ดำเนินการ ดังนี้

(๑) ต้องเก็บรักษาข้อมูลที่เกี่ยวข้องกับสิ่งที่ใช้ยืนยันตัวตนทั้งหมดที่เป็นหรือมีความสัมพันธ์ในแต่ละไอเดนทิตีของผู้ใช้บริการ โดยอย่างน้อยต้องเก็บรักษาข้อมูลวันและเวลาที่สร้างความสัมพันธ์ระหว่างสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตี และควรรวมถึงแหล่งของการเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน เช่น IP Address

(๒) ต้องเก็บรักษาข้อมูลเกี่ยวกับจำนวนครั้งของการยืนยันตัวตนผิดพลาดต่อเนื่อง เพื่อจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาด

(๓) ต้องตรวจสอบชนิดของสิ่งที่ใช้ยืนยันตัวตนให้เป็นไปตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน เช่น หากใช้สิ่งที่ใช้ยืนยันตัวตนหลายปัจจัยต้องใช้วิธีการยืนยันตัวตนแบบหลายปัจจัยเช่นกัน

(๔) ต้องเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนอย่างน้อย ๑ ปัจจัยและควรเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนอย่างน้อย ๒ ปัจจัย โดยที่ปัจจัยใดปัจจัยหนึ่งเป็นสิ่งที่ผู้ใช้บริการมี (Something You Have) เช่น โทเค็น (Token) เพื่อให้สามารถกู้คืนได้ กรณีที่เกิดการสูญหาย ถูกโจรกรรม เช่น ผู้ใช้บริการใช้อุปกรณ์ OTP ปัจจัยเดียวแล้วเกิดการเสียหาย จะใช้รหัสลับจดจำในการกู้คืน

(๕) ในกรณีที่การลงทะเบียนและเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนไม่สมบูรณ์ต้องใช้รหัสผ่านแบบชั่วคราว ทั้งนี้การใช้รหัสผ่านแบบชั่วคราวต้องไม่นำมาใช้ซ้ำ โดยจัดส่งไปยังหมายเลขโทรศัพท์หรืออีเมลของผู้สมัครใช้บริการ หรือใช้ข้อมูลชีวมิติที่ได้จัดเก็บไว้ตอนลงทะเบียนแบบพบเห็นต่อหน้าในการเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน

๕.๓.๒ การสูญหาย ถูกโจรกรรม และเสียหายของสิ่งที่ใช้ยืนยันตัวตน (Loss, Theft and Damage)

สิ่งที่ใช้ยืนยันตัวตนที่สูญหาย ถูกโจรกรรม หรือเสียหาย ถือว่าเป็นสิ่งที่ใช้ยืนยันตัวตนที่เสี่ยงต่อการใช้งานโดยผู้ไม่ประสงค์ดีในการนำสิ่งที่ใช้ยืนยันตัวตนไปใช้โดยไม่มีสิทธิ ดังนั้นผู้พิสูจน์และยืนยันตัวตนจึงควรให้ความสำคัญกับแนวปฏิบัติในกรณีสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกโจรกรรม และเสียหาย

โดยผู้พิสูจน์และยืนยันตัวตนดำเนินการ ดังนี้

(๑) ต้องจัดให้มีช่องทางสำหรับรายงานการสูญหาย ถูกโจรกรรม และเสียหายของสิ่งที่ใช้ยืนยันตัวตน

(๒) ควรจัดให้มีวิธีการยืนยันตัวตนสำรองหรือวิธีการอื่น ๆ ที่ใช้ตรวจสอบว่ารายงานการสูญหาย ถูกโจรกรรม และเสียหายของสิ่งที่ใช้ยืนยันตัวตน มาจากผู้ใช้บริการที่กล่าวอ้างจริง

(๓) ต้องระงับการใช้งาน เพิกถอน หรือทำลายสิ่งที่ใช้ยืนยันตัวตนทันที หลังจากตรวจพบว่าสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกโจรกรรม หรือเสียหาย

(๔) หลังจากสิ่งที่ใช้ยืนยันตัวตนถูกระงับการใช้งานอาจมีการกำหนดระยะเวลาของการเปิดใช้งานใหม่อีกครั้ง หากเกินจากระยะเวลาที่กำหนดจะไม่สามารถกลับมาใช้งานได้อีก

(๕) ต้องดำเนินการพิสูจน์ตัวตนผู้ใช้บริการใหม่อีกครั้ง แต่ไม่จำต้องพิสูจน์ตัวตนใหม่ทั้งหมด ทั้งนี้อาจตรวจสอบความสัมพันธ์ระหว่างตัวตนผู้ใช้บริการกับข้อมูลและหลักฐานแสดงตนที่ได้จัดเก็บไว้ในการลงทะเบียนและพิสูจน์ตัวตนไว้ก่อนหน้าด้วยวิธีการที่เหมาะสม

๕.๓.๓ การหมดอายุ (Expiration)

โดยผู้พิสูจน์และยืนยันตัวตนดำเนินการ ดังนี้

(๑) สิ่งที่ใช้ยืนยันตัวตนที่หมดอายุต้องไม่สามารถใช้ยืนยันตัวตนได้

(๒) เมื่อมีการยืนยันตัวตนโดยใช้สิ่งที่ใช้ยืนยันตัวตนที่หมดอายุ ควรแจ้งให้ผู้ใช้บริการทราบว่าการยืนยันตัวตนไม่สำเร็จเนื่องจากสิ่งที่ใช้ยืนยันตัวตนหมดอายุ

(๓) ควรเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนใหม่หรือต่ออายุการใช้งานสิ่งที่ใช้ยืนยันตัวตนในระยะเวลาที่เหมาะสมก่อนที่สิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการจะหมดอายุ

(๔) ต้องเพิกถอนหรือทำลายสิ่งที่ใช้ยืนยันตัวตนเดิม เมื่อผู้ใช้บริการได้รับและใช้สิ่งที่ใช้ยืนยันตัวตนใหม่

๕.๓.๔ การเพิกถอน (Revocation)

การเพิกถอนสิ่งที่ใช้ยืนยันตัวตน คือ การยุติความเชื่อมโยงระหว่างสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตีของผู้ใช้บริการ

โดยผู้พิสูจน์และยืนยันตัวตน ต้องเพิกถอนสิ่งที่ใช้ยืนยันตัวตนทันที เมื่อมีกรณีใดกรณีหนึ่งดังนี้

(๑) ไอเดนทิตีถูกเพิกถอน เช่น ผู้ใช้บริการเสียชีวิต ผู้ใช้บริการถูกตรวจพบว่ามีการหลอกลวงหรือปลอมแปลง หรือไม่แสดงตัวตนจริง

(๒) ผู้ใช้บริการต้องการเพิกถอนสิ่งที่ใช้ยืนยันตัวตนหรือยกเลิกการใช้บริการกับผู้พิสูจน์และยืนยันตัวตน

(๓) ในกรณีที่ตรวจพบในภายหลังว่าผู้ใช้บริการมีคุณสมบัติไม่ตรงตามเกณฑ์ที่ผู้พิสูจน์และยืนยันตัวตนกำหนด

๕.๔ การบริหารจัดการเซสชัน (Session Management)

การกำหนดเซสชัน อาจเริ่มตั้งแต่การยืนยันตัวตนไปจนถึงการสิ้นสุดการใช้งาน ทั้งนี้การยกเลิกเซสชันอาจเกิดขึ้นได้ เช่น การไม่มีกิจกรรมใด ๆ เกิดขึ้นในระยะเวลาที่กำหนด หรือถูกยกเลิกโดยผู้ใช้บริการ หากต้องการใช้บริการต่อจากเซสชันเดิมที่ถูกยกเลิกแล้ว ให้ผู้ใช้บริการยืนยันตัวตนซ้ำอีกครั้งเพื่อเข้าใช้งาน

๕.๔.๑ การเชื่อมโยงเซสชัน (Session Binding)

เซสชันจะเกิดขึ้นระหว่างแอปพลิเคชันของผู้ใช้บริการ (Session Subject) เช่น เว็บไซต์ ระบบปฏิบัติการ กับผู้ให้บริการภาครัฐหรือผู้พิสูจน์และยืนยันตัวตน (Session Host) ที่เข้าถึงโดยผู้ใช้บริการหลังจากยืนยันตัวตนสำเร็จ

ความลับของเซสชัน (Session Secret) ต้องใช้ร่วมกันระหว่างแอปพลิเคชันของผู้ใช้บริการกับบริการที่เข้าถึงเพื่อให้สามารถใช้งานได้อย่างต่อเนื่องจนถึงสิ้นสุดการใช้งาน โดยความลับของเซสชันจะต้องมีกลไกในการเข้ารหัส (Cryptographic Mechanism) ทั้งนี้ การเชื่อมโยงเซสชันต้องสอดคล้องกับคุณสมบัติตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนด้วย ความลับในการเชื่อมโยงเซสชัน มีดังนี้

(๑) ต้องสร้างขึ้นทันทีโดย Session Host หลังจากการยืนยันตัวตนสำเร็จ

(๒) ต้องสร้างขึ้นโดยวิธีการสุ่ม และประกอบด้วยอย่างน้อย ๖๔ บิต

(๓) ต้องลบหรือทำให้ใช้งานไม่ได้โดย Session Subject หลังจากที่ผู้ใช้บริการออกจากระบบ

(๔) ควรลบการเชื่อมโยงเซสชัน เมื่อผู้ใช้บริการออกจากระบบหรือเมื่อความลับหมดอายุการใช้งาน

(๕) ไม่ควรจัดเก็บเซสชัน ไว้ในสถานที่ที่ไม่ปลอดภัย เช่น HTML5 ซึ่งอาจเสี่ยงต่อการโจมตีแบบ Cross-site Scripting (XSS)

(๖) ต้องส่งและรับเซสชัน จากอุปกรณ์ผ่านช่องทางที่มีความปลอดภัย

(๗) ต้องตั้งเวลาหมดอายุไม่ให้ใช้งานได้ ดังนี้

- ๓๐ วัน สำหรับ AAL1
- ๑๒ ชั่วโมง หรือ ๓๐ นาที ที่ไม่มีกิจกรรมใด ๆ เกิดขึ้น สำหรับ AAL2

- ๑๒ ชั่วโมง หรือ ๑๕ นาที ที่ไม่มีกิจกรรมใด ๆ เกิดขึ้น สำหรับ AAL3

(๘) ต้องไม่สามารถใช้งานผ่านช่องทางการสื่อสารที่ไม่ปลอดภัย และเมื่อยืนยันตัวตนสำเร็จต้องไม่ลดระดับไปยังช่องทางการสื่อสารที่ไม่ปลอดภัย เช่น จาก HTTPS เป็น HTTP

๕.๔.๑.๑ เบราว์เซอร์คุกกี้ (Browser Cookies)

เบราว์เซอร์คุกกี้เป็นกลไกที่ใช้สำหรับสร้างเซสชัน และติดตามผู้ใช้บริการขณะที่เข้าใช้บริการ ควรกำหนด ดังนี้

- ต้องกำหนดให้มีการเข้าถึงคุกกี้ได้เฉพาะการเชื่อมต่อที่ใช้งาน HTTPS เท่านั้น
- ต้องระบุ Hostname และ Path ที่อนุญาตให้ใช้คุกกี้น้อยที่สุดเท่าที่จำเป็น
- ควรกำหนดให้ JavaScript ไม่สามารถเข้าถึงคุกกี้ได้ โดยการกำหนด Flag HttpOnly ให้กับคุกกี้
- ควรกำหนดระยะเวลาหมดอายุของคุกกี้

๕.๔.๑.๒ แอกเซสโทเค็น (Access Token)

แอกเซสโทเค็นใช้สำหรับอนุญาตให้แอปพลิเคชันเข้าถึงบริการภาครัฐในฐานะของผู้ใช้บริการหลังจากการยืนยันตัวตนสำเร็จ โดยผู้ให้บริการภาครัฐต้องไม่ถือว่าการแสดง OAuth Access Token เป็นการยืนยันตัวตนตามหลักการของดิจิทัลไอดี ซึ่งอาจต้องใช้องค์ประกอบอื่น ๆ เพิ่มเติมด้วย เนื่องจาก OAuth Access Token และ Refresh Token ที่เกี่ยวข้อง อาจคงสถานะการใช้งานได้หลังจากการสิ้นสุดเซสชันและผู้ใช้บริการได้ออกจากแอปพลิเคชันไปแล้ว

๕.๔.๑.๓ การระบุอุปกรณ์ (Device Identification)

วิธีการระบุอุปกรณ์ที่มีความปลอดภัย เช่น การใช้โพรโทคอล TLS หรือการเชื่อมโยงโทเค็น (Token Binding) หรือวิธีการอื่น ๆ อาจนำมาใช้สร้างเซสชันระหว่างผู้ใช้บริการกับบริการภาครัฐได้

๕.๔.๒ การยืนยันตัวตนซ้ำ (Reauthentication)

ความต่อเนื่องของเซสชันต้องขึ้นอยู่กับความลับของเซสชันที่ครอบครองในช่วงเวลาของการยืนยันตัวตนที่ออกโดยผู้พิสูจน์และยืนยันตัวตน และอาจมีการ Refresh Session

ความลับของเซสชันต้องไม่คงอยู่ถาวรและต้องไม่เก็บไว้หากมีการเริ่มใช้งาน (Restart) แอปพลิเคชันใหม่ หรือรีบูต (Reboot) เครื่องที่ให้บริการ

การยืนยันตัวตนซ้ำตามช่วงเวลาที่กำหนดของแต่ละระดับ AAL ต้องเกิดขึ้นเพื่อยืนยันว่าผู้ใช้บริการยังคงมีสถานะใช้งานอยู่ ก่อนที่เซสชันจะสิ้นสุดเนื่องจากหมดเวลาหรือด้วยเหตุผลอื่น ๆ ผู้ใช้บริการต้องยืนยันตัวตนซ้ำเพื่อต่ออายุการใช้งานเซสชันโดยมีวิธีการดังนี้

- ระดับ AAL1 : ยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนอย่างน้อยหนึ่งปัจจัย
- ระดับ AAL2 : ยืนยันตัวตนโดยใช้รหัสลับจดจำหรือชีวมิติ
- ระดับ AAL3 : ยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนทั้งหมด

เมื่อถึงเวลาที่กำหนดไว้ เซสชันควรถูกทำให้สิ้นสุดลง (Terminated) เช่น การออกจากระบบ ทั้งนี้ เมื่อเซสชันถูกทำให้สิ้นสุดลงแล้ว ผู้ใช้บริการจะต้องยืนยันตัวตนใหม่อีกครั้งโดยต้องมีการสร้างเซสชันใหม่ขึ้นมา

๕.๕ ภัยคุกคาม (Threats and Security Considerations)

นอกจากนี้ ในกระบวนการยืนยันตัวตนต้องคำนึงถึงภัยคุกคามที่อาจจะเกิดขึ้นได้ ที่อาจก่อให้เกิดความเสียหายแก่ระบบงานและข้อมูลต่าง ๆ ดังนี้

ตารางที่ ๓ ภัยคุกคามและการบรรเทาภัยคุกคามที่อาจเกิดขึ้นในขั้นตอนการยืนยันตัวตน

ภัยคุกคาม	รายละเอียด	ตัวอย่าง	การบรรเทาภัยคุกคามที่อาจเกิดขึ้น
การเดาออนไลน์ (Online Guessing)	เป็นวิธีการที่ผู้ไม่ประสงค์ดีพยายามเข้าระบบ (Login) ซ้ำ ๆ โดยทดลองเดาผลลัพธ์หรือค่าต่าง ๆ ที่จะสามารถผ่านเข้าไปยังระบบได้	การพยายามเข้าเว็บไซต์โดยลักลอบใช้ชื่อผู้ใช้งาน (Username) และทดลองใช้รหัสผ่าน (Password) ที่ผู้ใช้บริการอาจใช้บ่อย ๆ	ป้องกันไม่ให้ผู้ไม่ประสงค์ดีล่วงรู้ข้อมูลเฉพาะของผู้ใช้บริการ ที่ใช้เป็นข้อมูลลับในการยืนยันตัวตน ผู้พิสูจน์และยืนยันตัวตนควรคำนึงถึงระดับความยากง่ายของการสร้างข้อมูลลับ ความปลอดภัยของข้อมูลที่รับส่งผ่านช่องทางการยืนยันตัวตนและวิธีการบริหารจัดการอื่นๆ เช่น การใช้รหัสผ่านที่คาดเดายากและจำกัดจำนวนครั้งของความพยายามในการยืนยันตัวตนที่ไม่สำเร็จ
การส่งข้อมูลซ้ำ (Replay Attack)	เป็นวิธีการที่ผู้ไม่ประสงค์ดีสามารถนำข้อมูลที่เคยดักจับได้กลับมาใช้ยืนยันตัวตนเพื่อเข้าระบบเสมือนเป็นผู้ใช้บริการ	ผู้ไม่ประสงค์ดีอาจดักจับรหัสผ่าน (Password) จากผู้ใช้บริการในขณะยืนยันตัวตน และนำรหัสผ่านนั้นมาเข้าระบบในภายหลัง	ใช้ช่องทางการสื่อสารที่มีการตรวจสอบความเป็นปัจจุบันหรือมีการจำกัดเวลาของการใช้งานที่สอดคล้องกับช่วงเวลาในการยืนยันตัวตนปัจจุบัน
การขโมยเซสชัน (Session Hijack)	เป็นวิธีการที่ผู้ไม่ประสงค์ดีสามารถเข้าควบคุมเซสชัน ซึ่งอาจจะเป็นการแฝงตัวในการสื่อสารที่แลกเปลี่ยนข้อมูลการยืนยันตัวตนระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตนเพื่อเข้าควบคุมการสื่อสารนั้นไว้	ผู้ไม่ประสงค์ดีสามารถเข้าควบคุมการสื่อสารที่แลกเปลี่ยนข้อมูลการยืนยันตัวตนแล้วดักจับข้อมูลหรือคาดเดาค่า (Value) ของคุกกี้ที่ใช้ในการยืนยันตัวตน (Authentication Cookies) เพื่อระบุ HTTP Requests ของผู้ใช้บริการ	ใช้ช่องทางสื่อสารในการยืนยันตัวตนระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตนที่มีการควบคุมการรับส่งข้อมูลต่อช่วงเวลา (Per-session Data Transfer Protocol)

ภัยคุกคาม	รายละเอียด	ตัวอย่าง	การบรรเทาภัยคุกคามที่อาจเกิดขึ้น
การแอบดักจับข้อมูล (Eavesdropping)	เป็นวิธีการที่ผู้ไม่ประสงค์ดีลักลอบดักจับข้อมูลจากช่องทางการสื่อสาร เพื่อนำข้อมูลที่ได้ไปใช้ปลอมแปลงเป็นผู้ใช้บริการในการยืนยันตัวตนเข้าระบบ	แอบส่องรหัสลับจดจำเมื่อผู้ใช้งานพิมพ์รหัสลงบนแป้นพิมพ์ หรือใช้ซอฟต์แวร์ดักจับข้อมูลที่ได้มีการบันทึกการพิมพ์รหัสลงบนแป้นพิมพ์ (Keystroke)	ป้องกันไม่ให้ผู้ไม่ประสงค์ดีล่วงรู้ข้อมูลเฉพาะของผู้ใช้บริการ ที่ใช้เป็นข้อมูลลับในการยืนยันตัวตนโดยใช้ช่องทางการสื่อสารที่ป้องกันการดักจับข้อมูล เช่น Transport Layer Security (TLS) Protocol
การหลอกลวง (Phishing)	เป็นวิธีการที่ผู้ใช้บริการถูกล่อลวงโดยผู้ไม่ประสงค์ดี เพื่อให้เปิดเผยข้อมูลลับ ข้อมูลส่วนตัว หรือข้อมูลที่ใช้ในการยืนยันตัวตน โดยผู้ไม่ประสงค์ดีจะนำข้อมูลต่าง ๆ ที่ได้ไปปลอมตัวเป็นผู้ใช้บริการเพื่อยืนยันตัวตนเข้าใช้บริการภาครัฐ	การส่งอีเมลเพื่อล่อลวงให้ผู้ใช้บริการเข้าไปยังเว็บไซต์ที่ผู้ไม่ประสงค์ดีทำปลอมขึ้นมา โดยทำให้ผู้ใช้บริการคิดว่าเป็นเว็บไซต์จริง และล่อลวงให้ใส่ชื่อผู้ใช้งานและรหัสผ่าน (Username and Password) เพื่อเข้าระบบ เช่น เว็บไซต์ของผู้พิสูจน์และยืนยันตัวตนที่ผู้ใช้บริการมีบัญชี (Account) อยู่	ป้องกันไม่ให้ผู้ไม่ประสงค์ดีสามารถล่วงรู้หรือเรียนรู้ข้อมูลและพฤติกรรมส่วนตัวของผู้ใช้บริการ รวมถึงสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ
การลักลอบเป็นคนกลาง (Man-In-The-Middle)	เป็นวิธีการที่ผู้ไม่ประสงค์ดีแฝงตัวอยู่ในช่องทางการสื่อสารเพื่อลักลอบ ขัดขวาง แก้ไข หรือใช้เนื้อหาข้อมูลที่แลกเปลี่ยนกันในการยืนยันตัวตนระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน เพื่อให้ผู้ไม่ประสงค์ดีสามารถเข้าระบบได้ โดยปกติแล้วผู้ไม่ประสงค์ดีจะปลอมตัวเป็นผู้พิสูจน์และยืนยันตัวตนเพื่อหลอกผู้ใช้บริการ และในทำนองเดียวกันก็สามารถปลอมตัวเป็นผู้ใช้บริการเพื่อหลอกผู้พิสูจน์และยืนยันตัวตนได้เช่นกัน	ถ้าผู้ใช้บริการต้องการส่งข้อมูลไปยังผู้พิสูจน์และยืนยันตัวตนโดยมีการเข้ารหัสข้อมูลด้วยกุญแจสาธารณะของผู้พิสูจน์และยืนยันตัวตนในช่องทางการสื่อสาร ผู้ไม่ประสงค์ดีจะทำการสับเปลี่ยนกุญแจสาธารณะโดยส่งกุญแจสาธารณะของผู้ไม่ประสงค์ดีไปให้ผู้ใช้บริการและล่อลวงให้เข้ารหัสด้วยกุญแจสาธารณะนั้นแทน ซึ่งผู้ไม่ประสงค์ดีจะสามารถถอดรหัสข้อมูลนั้นได้ด้วยกุญแจส่วนตัวของผู้ไม่ประสงค์ดี	ตรวจสอบกระบวนการยืนยันตัวตน ให้แน่ใจว่าข้อมูลที่ถูกส่งระหว่างกันไม่สามารถดักจับได้ หากมีการส่งความลับ (Secret) หรือข้อมูลส่วนตัวผ่านทางอินเทอร์เน็ตต้องทำการเข้ารหัสก่อนทุกครั้ง ควรใช้เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) ในการยืนยันตัวตนระหว่างฝั่งของผู้ใช้บริการและฝั่งของผู้พิสูจน์และยืนยันตัวตน หรือใช้ช่องทางที่อนุญาตให้ผู้ใช้บริการเปิดเผยความลับไปยังผู้พิสูจน์และยืนยันตัวจริงเท่านั้น

๕.๖ ข้อกำหนดขั้นต่ำในการยืนยันตัวตนทางดิจิทัล (Minimum Requirement of Authentication)

เมื่อผู้ใช้บริการลงทะเบียนและพิสูจน์ตัวตน และได้รับสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ในการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตนเรียบร้อยแล้ว หากผู้ใช้บริการต้องการเข้าใช้บริการออนไลน์กับผู้ให้บริการภาครัฐ และผู้ให้บริการภาครัฐต้องการทราบว่าผู้ใช้บริการเป็นผู้ใด

สำหรับผู้ใช้บริการเคยลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตนที่ผู้ให้บริการภาครัฐเชื่อถือ ผู้ให้บริการภาครัฐจะนำผู้ใช้บริการ (Redirect) ไปยังหน้าต่างยืนยันตัวตนของผู้พิสูจน์และยืนยันตัวตนนั้น ผู้ใช้บริการต้องยืนยันตัวตนด้วยพิสูจน์ให้เห็นว่าตนครอบครองสิ่งที่ใช้ยืนยันตัวตนตามเกณฑ์วิธีที่ผู้พิสูจน์และยืนยันตัวตนกำหนด เมื่อตรวจสอบสิ่งที่ใช้ยืนยันตัวตนและสิ่งที่ใช้รับรองตัวตนเรียบร้อยแล้ว ผู้พิสูจน์และยืนยันตัวตนจะส่งผลการยืนยันตัวตนให้กับผู้ให้บริการภาครัฐ เพื่อให้ผู้ให้บริการภาครัฐนำไปใช้พิจารณาอนุญาตเข้าใช้บริการภาครัฐต่อไป

ข้อกำหนดขั้นต่ำในการยืนยันตัวตนทางดิจิทัล จำแนกตามกลุ่มการให้บริการภาครัฐ ดังนี้

(๑) กลุ่มการให้บริการข้อมูลพื้นฐาน จัดเป็นบริการที่ไม่มีความเสี่ยงหรือความเสี่ยงต่ำ จึง**ไม่จำเป็นต้องใช้ดิจิทัลไอดี**

(๒) กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ จัดเป็นบริการที่มีความเสี่ยงต่ำ สามารถใช้การยืนยันตัวตนในระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน **อย่างน้อยระดับที่ ๑**

(๓) กลุ่มการให้บริการธุรกรรม จัดเป็นบริการที่มีความเสี่ยงปานกลางถึงสูง โดยจำนวนและประเภทของปัจจัยของการยืนยันตัวตนมีผลกับระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน เพื่อให้มั่นใจว่าผู้ใช้บริการเป็นบุคคลที่ได้ลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตนจริง สามารถใช้การยืนยันตัวตนในระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน **อย่างน้อยระดับที่ ๒**

(๔) กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงาน จัดเป็นบริการที่มีความเสี่ยงสูง สามารถใช้การยืนยันตัวตนในระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน **อย่างน้อยระดับที่ ๒**

รายละเอียดแนวทางการกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนของกลุ่มการให้บริการภาครัฐ ดังตารางที่ ๔

ตารางที่ ๔ แนวทางการกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนของกลุ่มการให้บริการภาครัฐ

กลุ่มการให้บริการภาครัฐ	ระดับ AAL ขั้นต่ำ	การยืนยันตัวตน	ข้อกำหนด
กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ	AAL1	ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้	ชนิดของสิ่งที่ใช้ยืนยันตัวตนชนิดใดชนิดหนึ่งจากตัวเลือกต่อไปนี้ - รหัสลับจดจำ (Memorized Secret) - อุปกรณ์สื่อสารช่องทางอื่น (Out-of-Band Device) - อุปกรณ์ OTP ปัจจัยเดียว (Single-factor OTP Device) - ซอฟต์แวร์เข้ารหัสลับปัจจัยเดียว (Single-factor Cryptographic Software) - อุปกรณ์เข้ารหัสลับปัจจัยเดียว (Single-factor Cryptographic Device) - สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ในระดับ AAL2 และ AAL3
		การยืนยันตัวตนซ้ำ	อย่างน้อยทุก ๓๐ วัน
		การป้องกันการโจมตีโดยคนกลางของช่องทางที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน	จำเป็น
		การป้องกันการโจมตีแบบส่งข้อมูลซ้ำของสิ่งที่ใช้ยืนยันตัวตน	ไม่จำเป็น
		การป้องกันผู้พิสูจน์และยืนยันตัวตนปลอมของสิ่งที่ใช้ยืนยันตัวตน	ไม่จำเป็น

กลุ่มการให้บริการภาครัฐ	ระดับ AAL ขั้นต่ำ	การยืนยันตัวตน	ข้อกำหนด
- **กลุ่มการให้บริการธุรกรรม** - **กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงาน**	AAL2	ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้	ชนิดของสิ่งที่ใช้ยืนยันตัวตนชนิดใดชนิดหนึ่งจากตัวเลือกต่อไปนี้ - อุปกรณ์ OTP หลายปัจจัย (Multi-factor OTP Device) - ซอฟต์แวร์เข้ารหัสลับหลายปัจจัย (Multi-factor Cryptographic Software) - รหัสลับจดจำ (Memorized Secret) ร่วมกับอุปกรณ์สื่อสารช่องทางอื่น (Out-of-band Device) - รหัสลับจดจำ (Memorized Secret) ร่วมกับอุปกรณ์ OTP ปัจจัยเดียว (Single-factor OTP Device) - รหัสลับจดจำ (Memorized Secret) ร่วมกับซอฟต์แวร์เข้ารหัสลับปัจจัยเดียว (Single-factor Cryptographic Software) - รหัสลับจดจำ (Memorized Secret) ร่วมกับอุปกรณ์เข้ารหัสลับปัจจัยเดียว (Single-factor Cryptographic Device) - ชีวมิติ (Biometric) ร่วมกับชนิดของสิ่งที่ใช้ยืนยันตัวตนชนิดใดชนิดหนึ่งจากตัวเลือกข้างต้น - สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ในระดับ AAL3
		การยืนยันตัวตนซ้ำ	- อย่างน้อยทุก ๑๒ ชั่วโมง **หรือ** - ๓๐ นาทีหากไม่มีกิจกรรมใด ๆ เกิดขึ้น ผู้ใช้บริการอาจยืนยันตัวตนโดยใช้ ๑ ปัจจัย (รหัสลับจดจำหรือชีวมิติ)
		การป้องกันการโจมตีโดยคนกลางของช่องทางที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน	จำเป็น
		การป้องกันการโจมตีแบบส่งข้อมูลซ้ำ	จำเป็น

กลุ่มการให้บริการภาครัฐ	ระดับ AAL ขั้นต่ำ	การยืนยันตัวตน	ข้อกำหนด
		การป้องกันผู้พิสูจน์และยืนยันตัวตนปลอม	ไม่จำเป็น
	AAL3	ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้	ชนิดของสิ่งที่ใช้ยืนยันตัวตนชนิดใดชนิดหนึ่งจากตัวเลือกต่อไปนี้ - อุปกรณ์เข้ารหัสลับหลายปัจจัย (Multi-factor Cryptographic Device) - อุปกรณ์เข้ารหัสลับปัจจัยเดียว (Single-factor Cryptographic Device) ร่วมกับ รหัสลับจดจำ (Memorized Secret) - อุปกรณ์ OTP หลายปัจจัย (Multi-factor OTP Device) ร่วมกับอุปกรณ์เข้ารหัสลับปัจจัยเดียว (Single-factor Cryptographic Device) - อุปกรณ์ OTP หลายปัจจัย (Multi-factor OTP Device) ร่วมกับซอฟต์แวร์เข้ารหัสลับปัจจัยเดียว (Single-factor Cryptographic Software) - อุปกรณ์ OTP ปัจจัยเดียว (Single-factor OTP Device) ร่วมกับซอฟต์แวร์เข้ารหัสลับหลายปัจจัย (Multi-factor Cryptographic Software) - อุปกรณ์ OTP ปัจจัยเดียว (Single-factor OTP Device) ร่วมกับซอฟต์แวร์เข้ารหัสลับปัจจัยเดียว (Single-factor Cryptographic Software) และรหัสลับจดจำ (Memorized Secret)
		การยืนยันตัวตนซ้ำ	- อย่างน้อยทุก ๑๒ ชั่วโมง **หรือ** - ๑๕ นาทีหากไม่มีกิจกรรมใด ๆ เกิดขึ้น ผู้ใช้บริการต้องยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนทั้งหมด

กลุ่มการให้บริการภาครัฐ	ระดับ AAL ขั้นต่ำ	การยืนยันตัวตน	ข้อกำหนด
		การป้องกันการโจมตีโดยคนกลางของช่องทางที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน	จำเป็น
		การป้องกันการโจมตีแบบส่งข้อมูลซ้ำ	จำเป็น
		การป้องกันผู้พิสูจน์และยืนยันตัวตนปลอม	จำเป็น

๖. การพิจารณาการคุ้มครองข้อมูลส่วนบุคคล (Privacy Considerations)

การพิจารณาการคุ้มครองข้อมูลส่วนบุคคล ควรพิจารณา ดังนี้

๖.๑ การจัดเก็บข้อมูลเท่าที่จำเป็น (Data Minimization)

ตามพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๒๒ กำหนดให้มีการเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล โดยต้องมีแนวทางในการดำเนินการเพื่อประกันการจัดเก็บข้อมูลเท่าที่จำเป็นทั้งในแง่ของประเภทข้อมูลและระยะเวลาการจัดเก็บข้อมูล ซึ่งการจัดเก็บข้อมูลเท่าที่จำเป็นจะเป็นการลดความเสี่ยงที่อาจเกิดขึ้นได้จากการใช้งานหรือเข้าถึงโดยไม่ได้รับอนุญาต

ทั้งนี้ ในการจัดเก็บข้อมูลส่วนบุคคล ผู้พิสูจน์และยืนยันตัวตนควรพิจารณาถึงการดำเนินการคุ้มครองข้อมูลส่วนบุคคล ให้สอดคล้องกับกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลเป็นสำคัญ

๖.๒ เอกสารแจ้งข้อมูลและเอกสารแสดงความยินยอม (Privacy Notice and Consent)

ตามพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๑๙ ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้พิสูจน์และยืนยันตัวตนต้องแจ้งวัตถุประสงค์ของการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว

ทั้งนี้ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลต้องเป็นไปตามแบบและข้อความตามที่กฎหมายกำหนด ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้พิสูจน์และยืนยันตัวตนต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้ ในการเข้าทำสัญญา ซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญา ซึ่งรวมถึงการให้บริการนั้น ๆ เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่าย เช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล ทั้งนี้ การถอนความยินยอมย่อมไม่ส่งผลกระทบต่อ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปแล้วโดยชอบ

ในกรณีถอนความยินยอมผู้พิสูจน์และยืนยันตัวตนต้องแจ้งส่งผลกระทบจากการถอนความยินยอมให้เจ้าของข้อมูลส่วนบุคคลทราบ ทั้งนี้ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ไม่เป็นไปตามที่กฎหมายกำหนด จะไม่มีผลผูกพันกับเจ้าของข้อมูลส่วนบุคคล และผู้พิสูจน์และยืนยันตัวตนไม่สามารถเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้

๖.๓ การคุ้มครองความเป็นส่วนบุคคล (Privacy Control)

ผู้พิสูจน์และยืนยันตัวตนควรจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยด้านการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม โดยครอบคลุมถึงการแจ้งเตือน การแก้ไข หรือการพิจารณาอื่น ๆ ที่สำคัญ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือ

โดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม รวมถึงการขอความยินยอมต้องทำเป็นลายลักษณ์อักษรที่ชัดเจน และทำผ่านระบบอิเล็กทรอนิกส์ได้

๖.๔ การใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็น (Use Limitation)

การใช้และประมวลผลข้อมูลส่วนบุคคลต้องเป็นไปตามวัตถุประสงค์และการแสดงความยินยอมของเจ้าของข้อมูลส่วนบุคคลในเรื่องนั้น ๆ หากใช้ข้อมูลชุดเดียวกันเพื่อประมวลผลหลายวัตถุประสงค์ ต้องให้เจ้าของข้อมูลมีทางเลือกได้ว่ายินยอมสำหรับกรณีใดบ้าง ในกรณีที่ไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล มีดังนี้

(๑) เพื่อจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษา วิจัย หรือสถิติ ที่มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม

(๒) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

(๓) เพื่อปฏิบัติตามสัญญาที่เจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(๔) เพื่อปฏิบัติตามหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

(๕) เพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

(๖) เพื่อปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

ทั้งนี้ ผู้พิสูจน์และยืนยันตัวตนควรประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล และควรวัดผลการบริหารจัดการให้เป็นไปตามวัตถุประสงค์ที่ตั้งไว้ไม่ให้สูงเกินจากที่กำหนดไว้ภายใต้บริการนั้น

๖.๕ การแก้ไขข้อมูลส่วนบุคคล (Redress)

ผู้พิสูจน์และยืนยันตัวตนต้องมีมาตรการที่มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม

๖.๖ การประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล (Privacy Risk Assessment)

ผู้พิสูจน์และยืนยันตัวตน ควรพิจารณาดังนี้

(๑) โอกาสที่จะเกิดการดำเนินงานที่สร้างหรือก่อให้เกิดปัญหาต่อผู้สมัครใช้บริการ หรือผู้ใช้บริการในระบบ เช่น ขั้นตอนการตรวจสอบหรือการจัดเก็บบันทึกข้อมูลส่วนบุคคลอาจทำให้เกิดการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

(๒) ผลกระทบเมื่อเกิดปัญหาขึ้น

ผู้พิสูจน์และยืนยันตัวตนควรมีแนวทางในการตอบสนองต่อความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลที่รวมถึงการยอมรับความเสี่ยง การบรรเทาความเสี่ยง และการแบ่งปันความเสี่ยง ทั้งนี้การ

ให้ความยินยอมของผู้ใช้บริการถือเป็นรูปแบบหนึ่งของการแบ่งปันความเสี่ยง ซึ่งใช้ได้เฉพาะกับผู้ใช้บริการที่ยอมรับข้อตกลงและเงื่อนไขการให้บริการที่เหมาะสมเพียงพอที่จะแบ่งปันความเสี่ยงได้

๖.๗ การดำเนินการให้สอดคล้องกับการคุ้มครองข้อมูลส่วนบุคคล (Privacy Compliance)

ผู้พิสูจน์และยืนยันตัวตนควรพิจารณาถึงการดำเนินการให้สอดคล้องกับการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดไว้ เช่น กฎหมาย ข้อกำหนด ข้อตกลง นโยบาย แนวปฏิบัติ เพื่อที่จะประเมินและบรรเทาความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล รวมถึงการให้คำแนะนำกับหน่วยงานที่เกี่ยวข้องเพื่อปฏิบัติ

๗. แนวทางการนำไปใช้ (Usability Considerations)

ในการพิสูจน์และยืนยันตัวตนทางดิจิทัลสามารถกำหนดข้อตกลงร่วมกันในการพิสูจน์และยืนยันตัวตนทางดิจิทัลระหว่างผู้พิสูจน์และยืนยันตัวตน ผู้ให้บริการภาครัฐ และแหล่งให้ข้อมูลที่น่าเชื่อถือ ดังนี้

๗.๑ สำหรับผู้พิสูจน์และยืนยันตัวตน (Identity Provider: IdP)

๗.๑.๑ กำหนดรูปแบบของการพิสูจน์และยืนยันตัวตนทางดิจิทัลให้สอดคล้องกับระดับความน่าเชื่อถือ

ต้องกำหนดรูปแบบของการพิสูจน์และยืนยันตัวตนทางดิจิทัลให้สอดคล้องกับระดับความน่าเชื่อถือ โดยจัดให้มีทรัพยากรที่เพียงพอ เหมาะสม มีความน่าเชื่อถือ และมีมาตรการหรือระบบรักษาความมั่นคงปลอดภัย เช่น กระบวนการ ระบบ เทคโนโลยี บุคลากร สถานที่ รายละเอียดตามแนวทางฯ ฉบับนี้

๗.๑.๒ ดำเนินการทำความรู้จักผู้ใช้บริการ

ต้องดำเนินการทำความรู้จักผู้ใช้บริการ รายละเอียดตามข้อ ๓. การทำความรู้จักผู้ใช้บริการ

๗.๑.๓ ดำเนินการตามข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลตามกลุ่มการให้บริการภาครัฐ

ต้องดำเนินการตามข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล รายละเอียดตามข้อ ๔. ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล ดังนี้

- รวบรวมข้อมูลเพื่อระบุตัวตน
- ตรวจสอบหลักฐานแสดงตน
- ตรวจสอบตัวบุคคล

ทั้งนี้ต้องพิจารณาถึงการคุ้มครองข้อมูลส่วนบุคคล รายละเอียดตามข้อ ๖.

๗.๑.๔ ดำเนินการตามข้อกำหนดการยืนยันตัวตนทางดิจิทัลตามกลุ่มการให้บริการภาครัฐ

ต้องดำเนินการตามข้อกำหนดของการยืนยันตัวตนทางดิจิทัล รายละเอียดตามข้อ ๕. ข้อกำหนดการยืนยันตัวตนทางดิจิทัล

ทั้งนี้ต้องพิจารณาถึงการคุ้มครองข้อมูลส่วนบุคคล รายละเอียดตามข้อ ๖.

๗.๑.๕ ต้องปฏิบัติตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนดโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และถูกบังคับภายใต้พระราชกฤษฎีกากำหนดให้การประกอบธุรกิจบริการเกี่ยวกับระบบพิสูจน์และยืนยันตัวตนทางดิจิทัลซึ่งตราขึ้นตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๗.๑.๖ ประกาศข้อกำหนดให้ผู้ที่เกี่ยวข้องในกระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัลทราบโดยทั่วกัน

๗.๒ สำหรับผู้ให้บริการภาครัฐ

การเลือกใช้รูปแบบ วิธีการ รวมถึงระดับความน่าเชื่อถือที่เหมาะสมกับบริการภาครัฐนั้นมีความสำคัญอย่างยิ่ง ดังนั้นการออกแบบและการนำไปใช้ ต้องคำนึงถึงกระบวนการ [๗] ดังนี้

๗.๒.๑ กำหนดความต้องการและระบบของหน่วยงานของรัฐที่ต้องการใช้ดิจิทัลไอดี

ต้องกำหนดความต้องการและระบบของบริการภาครัฐของหน่วยงานของตนที่ต้องการใช้ดิจิทัลไอดี ทั้งนี้ ผลลัพธ์ที่ได้จะนำใช้ในการวิเคราะห์และประเมินความเสี่ยง โดยพิจารณา ดังนี้

(๑) กำหนดบริการภาครัฐอย่างชัดเจนว่ามีบริการใดบ้างที่จำเป็นต้องใช้ข้อมูลส่วนบุคคลในการให้บริการ

(๒) กำหนดบริการภาครัฐอย่างชัดเจนว่าจำเป็นต้องลงทะเบียนและพิสูจน์ตัวตนหรือไม่

(๓) กำหนดผู้เกี่ยวข้อง บทบาท และหน้าที่

(๔) กำหนดช่องทางดิจิทัลที่ใช้ในการรับส่งข้อมูล เช่น อีเมล หมายเลขโทรศัพท์

๗.๒.๒ ประเมินความเสี่ยง

ต้องพิจารณาถึงผลกระทบ ระดับความรุนแรง และความสูญเสียที่อาจเกิดขึ้นได้หากการพิสูจน์และยืนยันตัวตนผิดพลาด และควรมุ่งเน้นที่กระบวนการธุรกรรมออนไลน์เป็นหลัก รายละเอียดตามแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม ข้อ ๗.๓ ความเสี่ยงและผลกระทบ

๗.๒.๓ กำหนดระดับความน่าเชื่อถือ

ต้องนำผลการจัดระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือของไอเดนทิตีเมื่อเกิดข้อผิดพลาดในการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลจากข้อ ๗.๒.๒ มาใช้พิจารณาระดับความน่าเชื่อถือของไอเดนทิตี รายละเอียดตามแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม ข้อ ๘. การกำหนดระดับความน่าเชื่อถือของไอเดนทิตี

และต้องนำผลการจัดระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนเมื่อเกิดข้อผิดพลาดในการยืนยันตัวตนทางดิจิทัลจากข้อ ๗.๒.๒ มาใช้พิจารณาระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน รายละเอียดตามแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม ข้อ ๙. การกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

๗.๒.๔ เลือกรูปแบบ และวิธีการลงทะเบียน พิสูจน์ตัวตน และยืนยันตัวตนทางดิจิทัล

พิจารณาจัดรูปแบบการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลสำหรับบริการภาครัฐ โดยผู้พิสูจน์และยืนยันตัวตนจะเป็นผู้รับผิดชอบดูแลเกี่ยวกับการรับลงทะเบียน การพิสูจน์ตัวตน และบริหารจัดการสิ่งที่ใช้รับรองตัวตน ซึ่งเชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ โดยต้องมีการทำความรู้จักผู้ใช้บริการ รายละเอียดตามข้อ ๓. การทำความรู้จักผู้ใช้บริการ การรวบรวมข้อมูลเพื่อระบุตัวตน การตรวจสอบหลักฐานแสดงตน การตรวจสอบตัวบุคคล หรือการตรวจสอบช่องทางการติดต่อตามแต่ละระดับความน่าเชื่อถือ เพื่อกำหนดวิธีการลงทะเบียน ข้อ ๔. ข้อกำหนดการลงทะเบียนและพิสูจน์

ตัวตนทางดิจิทัล รวมถึงเลือกปัจจัยและชนิดของสิ่งที่ใช้ยืนยันตัวตนที่เหมาะสม รายละเอียดตามข้อ ๕. ข้อกำหนดการยืนยันตัวตนทางดิจิทัล

๗.๒.๕ ทบทวนความถูกต้องเหมาะสม

ต้องทบทวนถึงองค์ประกอบและความพร้อมทั้งหมดก่อนดำเนินการในกระบวนการพิสูจน์และยืนยันตัวตน นอกจากนี้ควรจะพิจารณาในเรื่องของค่าใช้จ่ายและผลประโยชน์ก่อนตัดสินใจดำเนินการต่าง ๆ รวมถึงควรประเมินระบบและเทคโนโลยีที่ใช้ในการพิสูจน์และยืนยันตัวตนเป็นประจำ

๗.๓ สำหรับแหล่งให้ข้อมูลที่น่าเชื่อถือ (Authoritative Source: AS)

๗.๓.๑ อนุญาตให้เข้าถึงข้อมูลส่วนบุคคล

ก่อนที่แหล่งให้ข้อมูลที่น่าเชื่อถือจะให้ข้อมูลกับผู้พิสูจน์และยืนยันตัวตนต้องตรวจสอบว่าผู้สมัครใช้บริการได้แสดงความยินยอมกับผู้พิสูจน์และยืนยันตัวตนดังกล่าวแล้ว และต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยที่เหมาะสมและรับส่งข้อมูลผ่านช่องทางที่มีความปลอดภัย

๗.๓.๒ ส่งผลการตรวจสอบข้อมูลของการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล

เมื่อผู้ใช้บริการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล แหล่งให้ข้อมูลที่น่าเชื่อถือจะตรวจสอบข้อมูลหรือสถานะของหลักฐานแสดงตนของผู้ใช้บริการตามการร้องขอจากผู้พิสูจน์และยืนยันตัวตน และส่งผลการตรวจสอบข้อมูลกลับไปยังผู้พิสูจน์และยืนยันตัวตน

บรรณานุกรม

[๑] National Institute of Standards and Technology, US Department of Commerce. (2017). *NIST Special Publication 800-63-3 – Digital Identity Guidelines*.

[๒] National Institute of Standards and Technology, US Department of Commerce. (2017). *NIST Special Publication 800-63A – Digital Identity Guidelines – Enrollment and Identity Proofing*.

[๓] National Institute of Standards and Technology, US Department of Commerce. (2017). *NIST Special Publication 800-63B – Digital Identity Guidelines – Authentication and Lifecycle Management*.

[๔] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (๒๕๖๑). *ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์*.

[๕] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (๒๕๖๑). *ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน*.

[๖] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (๒๕๖๑). *ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน*.

[๗] Department of Finance and Deregulation, Australian Government Information Management Office. (2009). *The National e-Authentication Framework*.

[๘] ประมวลกฎหมายอาญา.

[๙] Department of Economic and Social Affairs, United Nations, New York. (2012). *United Nations E-Government Survey 2012.*

[๑๐] ประกาศธนาคารแห่งประเทศไทย ที่ สนส. ๑๙/๒๕๖๒. (๒๕๖๒). เรื่อง หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน ประกาศ ณ วันที่ ๒ กันยายน พ.ศ. ๒๕๖๒ คัดจากราชกิจจานุเบกษา เล่มที่ ๑๓๖ ตอนพิเศษ ๒๑๙ ง วันที่ ๒ กันยายน ๒๕๖๒.

[๑๑] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (๒๕๖๑). *ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทำธุรกรรมแบบพบเห็นลูกค้าต่อหน้าสำหรับธนาคาร*.