ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล

เรื่อง มาตรฐานและหลักเกณฑ์การจัดทำกระบวนการและการดำเนินงานทางดิจิทัล
ว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

ตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ มีวัตถุประสงค์เพื่อให้การบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน ให้หน่วยงานของรัฐจัดให้มีการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัล โดยมีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล ประกอบกับให้เป็นตามพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม เพื่อส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือ และมีผลทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติ รวมทั้งให้หน่วยงานต่าง ๆ เกิดการพัฒนาทางเทคโนโลยีและส่งเสริมการใช้ธุรกรรมอิเล็กทรอนิกส์ให้สอดคล้องตามมาตรฐานที่กำหนด

เพื่อให้การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัลเป็นไปตามวัตถุประสงค์ดังกล่าวข้างต้น โดยที่พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ มาตรา ๑๒ (๒) กำหนดให้หน่วยงานของรัฐจัดทำกระบวนการหรือการดำเนินงานทางดิจิทัลเพื่อการบริหารราชการแผ่นดินและการให้บริการประชาชน กระบวนการหรือการดำเนินงานทางดิจิทัลนั้นต้องทำงานร่วมกันได้ตามมาตรฐาน ข้อกำหนด และหลักเกณฑ์ที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนดเพื่อให้มีความสอดคล้องและเชื่อมโยงระหว่างหน่วยงานของรัฐแห่งอื่นได้ ประกอบมาตรา ๑๒ (๔) จัดให้มีระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล และตามพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ (ฉบับที่ ๔) พ.ศ. ๒๕๖๒ หมวด ๓/๑ ระบบการพิสูจน์และการยืนยันตัวตนทางดิจิทัล เพื่อกำกับดูแลการพิสูจน์และยืนยันตัวตนทางดิจิทัลให้มีความน่าเชื่อถือและปลอดภัย จึงจำเป็นต้องกำหนดมาตรฐานและหลักเกณฑ์การจัดทำกระบวนการและการดำเนินงานทางดิจิทัลว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

อาศัยอำนาจตามความในมาตรา ๔ และมาตรา ๗ (๓) (๙) มาตรา ๑๒ (๒) (๔) แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ คณะกรรมการพัฒนารัฐบาลดิจิทัล ในคราวการประชุมครั้งที่ ๒/๒๕๖๔ วันที่ ๑๓ เดือนพฤษภาคม พ.ศ. ๒๕๖๔ จึงมีมติให้ออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การจัดทำกระบวนการและการดำเนินงานทางดิจิทัลว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย”

ข้อ ๒ ในประกาศนี้

“บริการภาครัฐ” หมายความว่า การดำเนินการอย่างหนึ่งอย่างใดที่หน่วยงานของรัฐจัดทำหรือจัดให้มีขึ้นหรือที่มอบอำนาจให้เอกชนดำเนินการแทนเพื่ออำนวยความสะดวกหรือตอบสนองความต้องการของประชาชน

“ไอเดนทิตี” (identity หรือ ID) หมายความว่า คุณลักษณะ หรือชุดของคุณลักษณะที่ใช้ระบุตัวบุคคลในบริบทที่กำหนด

“ดิจิทัลไอดี” (digital identity หรือ digital ID) หมายความว่า คุณลักษณะ หรือชุดของคุณลักษณะที่ถูกรวบรวมและบันทึกในรูปแบบดิจิทัล ซึ่งสามารถใช้ระบุตัวบุคคลในบริบทที่กำหนดและสามารถใช้ทำธุรกรรมอิเล็กทรอนิกส์

“ผู้พิสูจน์และยืนยันตัวตน” (identity provider) หมายความว่า บุคคลหรือหน่วยงานที่น่าเชื่อถือซึ่งทำหน้าที่

(๑) รับลงทะเบียนและพิสูจน์ตัวตน และ

(๒) บริหารจัดการสิ่งที่ใช้รับรองตัวตน ซึ่งเชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ

โดยผู้พิสูจน์และยืนยันตัวตนอาจบริหารจัดการสิ่งที่ใช้รับรองตัวตนเพื่อใช้ภายในองค์กรหรือใช้ภายนอกองค์กรก็ได้

“ผู้ให้บริการภาครัฐ” (relying party) หมายความว่า หน่วยงานของรัฐที่ให้บริการภาครัฐหรืออนุญาตให้เข้าถึงข้อมูลหรือระบบบริการภาครัฐ โดยอาศัยสิ่งที่ใช้ยืนยันตัวตนและผลการยืนยันตัวตนหรือสิ่งที่ใช้รับรองตัวตนจากผู้พิสูจน์และยืนยันตัวตน

“แหล่งให้ข้อมูลที่น่าเชื่อถือ” (authoritative source) หมายความว่า หน่วยงานที่มีความน่าเชื่อถือและสามารถเข้าถึงหรือมีข้อมูลที่ถูกต้อง ซึ่งทำหน้าที่

(๑) ตรวจสอบข้อมูลหรือสถานะของหลักฐานแสดงตนของผู้ใช้บริการตามการร้องขอจากผู้พิสูจน์และยืนยันตัวตน หรือ

(๒) อนุญาตให้ผู้ให้บริการภาครัฐเข้าถึงข้อมูลที่น่าเชื่อถือหรือข้อมูลส่วนบุคคลซึ่งได้รับความยินยอมจากผู้ใช้บริการ

“ผู้สมัครใช้บริการ” (applicant) หมายความว่า บุคคลที่สมัครใช้บริการพิสูจน์และยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน

“ผู้ใช้บริการ” (subscriber) หมายความว่า ผู้สมัครใช้บริการที่ผ่านการลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตน และได้รับสิ่งที่ใช้ยืนยันตัวตนสำหรับใช้ยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน

“การลงทะเบียน” (enrolment) หมายความว่า กระบวนการที่ผู้สมัครใช้บริการลงทะเบียนเป็นผู้ใช้บริการของผู้พิสูจน์และยืนยันตัวตน

“การพิสูจน์ตัวตน” (identity proofing) หมายความว่า กระบวนการที่ผู้พิสูจน์และยืนยันตัวตนรวบรวมข้อมูลตรวจสอบหลักฐานแสดงตน และตรวจสอบตัวตนของผู้สมัครใช้บริการ

“การยืนยันตัวตน” (authentication) หมายความว่า กระบวนการที่ผู้ใช้บริการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตนว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างด้วยการใช้สิ่งที่ใช้ยืนยันตัวตน

“สิ่งที่ใช้ยืนยันตัวตน” (authenticator) หมายความว่า สิ่งที่ผู้ใช้บริการครอบครองเพื่อใช้ในการยืนยันตัวตนโดยสิ่งที่ใช้ยืนยันตัวตนจะมีปัจจัยของการยืนยันตัวตนอย่างน้อยหนึ่งปัจจัย

“สิ่งที่ใช้รับรองตัวตน” (credential) หมายความว่า เอกสาร วัตถุ หรือกลุ่มข้อมูลที่เชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตน

“คุณลักษณะ” (attribute) หมายความว่า ลักษณะหรือคุณสมบัติที่ใช้ระบุตัวบุคคล

หมวด ๑
บททั่วไป

ข้อ ๓ เพื่อให้การพิสูจน์และยืนยันตัวตนทางดิจิทัล มีความน่าเชื่อถือ พร้อมใช้ ตรวจสอบได้ และเป็นไปตามที่กฎหมายกำหนด โดยพิจารณาถึงการคุ้มครองข้อมูลส่วนบุคคลเป็นสำคัญ ให้ผู้พิสูจน์และยืนยันตัวตน ผู้ให้บริการภาครัฐ และแหล่งให้ข้อมูลที่น่าเชื่อถือ ดำเนินการ ดังต่อไปนี้

(๑) จัดให้มีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยให้เป็นไปตามกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

(๒) จัดให้มีข้อตกลงในการดำเนินการและปฏิบัติตามข้อตกลงนั้น

(๓) ให้ความสำคัญและบริหารความเสี่ยงให้เหมาะสมกับระดับความเสี่ยงของบริการภาครัฐโดยพิจารณาถึงผลกระทบที่อาจเกิดขึ้น เพื่อกำหนดวิธีการบรรเทาความเสียหายที่อาจเกิดขึ้น

ผู้พิสูจน์และยืนยันตัวตน ผู้ให้บริการภาครัฐ และแหล่งให้ข้อมูลที่น่าเชื่อถือที่เป็นหน่วยงานของรัฐ ให้จัดทำธรรมาภิบาลข้อมูลภาครัฐและดำเนินการให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐที่เกี่ยวข้องกับกระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐด้วย

หมวด ๒
การพิสูจน์และยืนยันตัวตนทางดิจิทัล

ข้อ ๔ ให้ผู้พิสูจน์และยืนยันตัวตนดำเนินการ ดังต่อไปนี้

(๑) กำหนดรูปแบบของการพิสูจน์และยืนยันตัวตนทางดิจิทัล และจัดสรรบุคลากร ระบบเทคโนโลยีที่จำเป็น ให้สอดคล้องกับระดับความน่าเชื่อถือ

(๒) กำหนดนโยบายและกระบวนการปฏิบัติงานภายในที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ชัดเจนเป็นลายลักษณ์อักษร โดยต้องทบทวน สื่อสาร ทำความเข้าใจ สร้างความตระหนักให้กับเจ้าหน้าที่ที่ได้รับการฝึกอบรมหรือบุคลากรที่เกี่ยวข้องให้เห็นถึงความสำคัญ และปฏิบัติตาม

นโยบายและกระบวนการปฏิบัติงานภายในหรือหน่วยงานกำกับดูแลที่เกี่ยวข้อง รวมถึงต้องสื่อสาร ทำความเข้าใจและให้ความรู้กับผู้ใช้บริการด้วย

(๓) กรณีที่ผู้พิสูจน์และยืนยันตัวตนเป็นหน่วยงานของรัฐให้ดำเนินการตามข้อกำหนดการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามมาตรฐานและหลักเกณฑ์นี้ หากผู้พิสูจน์และยืนยันตัวตนเป็นหน่วยงานของเอกชนให้ดำเนินการตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

(๔) จัดให้มีการขอความยินยอมของผู้สมัครใช้บริการ โดยต้องแจ้งวัตถุประสงค์ของการจัดเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลด้วย

(๕) จัดให้มีการแสดงตนและรวบรวมข้อมูลเพื่อระบุตัวตนที่จำเป็นจากผู้สมัครใช้บริการเพื่อแยกแยะว่าไอเดนทิตีของผู้สมัครใช้บริการมีเพียงหนึ่งเดียว และมีความเฉพาะเจาะจงภายในบริบทของผู้ใช้บริการทั้งหมดที่ผู้พิสูจน์และยืนยันตัวตนดูแล

(๖) ตรวจสอบหลักฐานแสดงตนของผู้สมัครใช้บริการ เพื่อตรวจสอบความแท้จริง สถานะการใช้งาน และความถูกต้องของหลักฐานแสดงตน และตรวจสอบข้อมูลในหลักฐานแสดงตนว่าเป็นของบุคคลที่มีตัวตนอยู่จริง

(๗) ตรวจสอบตัวบุคคลของผู้สมัครใช้บริการที่แสดงหลักฐานแสดงตนว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างจริง โดยอาจตรวจสอบช่องทางติดต่อว่าเป็นเจ้าของช่องทางที่ใช้ในการติดต่อ และสามารถติดต่อหรือส่งข้อมูลไปยังผู้สมัครใช้บริการผ่านช่องทางดังกล่าวได้จริง

(๘) เก็บรักษาข้อมูลและหลักฐานแสดงตน รวมถึงภาพและเสียง (ถ้ามี) และการบันทึกเหตุการณ์และรายละเอียดการทำธุรกรรมเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยระยะเวลาการเก็บรักษาและการบันทึกดังกล่าวให้เป็นไปตามกฎหมาย ข้อบังคับ หรือแนวนโยบายที่เกี่ยวข้อง

(๙) ดำเนินการตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนดตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

(๑๐) ประกาศข้อกำหนดให้ผู้ที่เกี่ยวข้องในกระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัลทราบโดยทั่วกัน

ข้อ ๕ ให้ผู้ให้บริการภาครัฐดำเนินการ ดังต่อไปนี้

(๑) กำหนดความต้องการและระบบของหน่วยงานที่ต้องการใช้ดิจิทัลไอดี

(๒) ประเมินความเสี่ยงเพื่อพิจารณาถึงผลกระทบ ระดับความรุนแรง และความสูญเสียที่อาจเกิดขึ้นได้หากการพิสูจน์หรือยืนยันตัวตนผิดพลาด

(๓) นำผลการจัดระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือทั้งระดับความน่าเชื่อถือของไอเดนทิตีและระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

(๔) เลือกรูปแบบ และวิธีการลงทะเบียน การพิสูจน์ตัวตนและยืนยันตัวตนทางดิจิทัล รวมถึงกำหนดเงื่อนไขให้สอดคล้องตามข้อกำหนดในแต่ละระดับความน่าเชื่อถือตามกลุ่มให้บริการภาครัฐและแจ้งให้ทราบล่วงหน้า

ข้อ ๖ ให้แหล่งให้ข้อมูลที่น่าเชื่อถือตรวจสอบข้อมูลหรือสถานะของหลักฐานแสดงตนของผู้สมัครใช้บริการตามการร้องขอจากผู้พิสูจน์และยืนยันตัวตน และส่งผลการตรวจสอบข้อมูลกลับไปยังผู้พิสูจน์และยืนยันตัวตน

บทเฉพาะกาล

ข้อ ๗ ในระยะเริ่มแรก มิให้นำมาตรฐานและหลักเกณฑ์ตามประกาศนี้มาใช้บังคับกับผู้พิสูจน์และยืนยันตัวตน ผู้ให้บริการภาครัฐ และแหล่งให้ข้อมูลที่น่าเชื่อถือ จนกว่าจะพ้นกำหนดสองปีนับแต่วันที่ประกาศนี้มีผลใช้บังคับ

ประกาศ ณ วันที่ ๑๖ กันยายน พ.ศ. ๒๕๖๔
ดอน ปรมัตถ์วินัย
รองนายกรัฐมนตรี
ประธานกรรมการพัฒนารัฐบาลดิจิทัล

มาตรฐานรัฐบาลดิจิทัล

DIGITAL GOVERNMENT STANDARD

มรด. ๑ - ๑ : ๒๕๖๔

DGS 1 - 1 : 2564

ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม

DIGITALIZATION: DIGITAL ID - OVERVIEW

เวอร์ชัน ๑.๐

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สำนักนายกรัฐมนตรี

มาตรฐานรัฐบาลดิจิทัล
ว่าด้วยแนวทางการจัดทำกระบวนการ และการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม

มรด. ๑ - ๑ : ๒๕๖๔

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
อาคารบางกอกไทยทาวเวอร์ ชั้น ๑๗
เลขที่ ๑๐๘ ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพมหานคร ๑๐๔๐๐
หมายเลขโทรศัพท์: ๐ ๒๖๑๒ ๖๐๐๐ โทรสาร: ๐ ๒๖๑๒ ๖๐๑๑, ๐ ๒๖๑๒ ๖๐๑๒

ประกาศโดย
คณะกรรมการพัฒนารัฐบาลดิจิทัล
วันที่ ๑๖ กันยายน ๒๕๖๔

คณะกรรมการพัฒนารัฐบาลดิจิทัล

ประธานกรรมการ

นายกรัฐมนตรี ประธานกรรมการ
มอบหมายและมอบอำนาจให้รองนายกรัฐมนตรี (นายดอน ปรมัตถ์วินัย)

กรรมการ

รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ปลัดสำนักนายกรัฐมนตรี
ปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ผู้อำนวยการสำนักงบประมาณ
เลขาธิการคณะกรรมการข้าราชการพลเรือน
เลขาธิการคณะกรรมการพัฒนาระบบราชการ
เลขาธิการสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ
กรรมการผู้ทรงคุณวุฒิในคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม
กรรมการผู้ทรงคุณวุฒิในคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
กรรมการผู้ทรงคุณวุฒิในคณะกรรมการข้อมูลข่าวสารของราชการ
กรรมการผู้ทรงคุณวุฒิในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
กรรมการผู้ทรงคุณวุฒิในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

กรรมการและเลขานุการ

ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ช่วยเลขานุการ

เจ้าหน้าที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะอนุกรรมการสถาปัตยกรรมและมาตรฐานการพัฒนารัฐบาลดิจิทัล

ประธานอนุกรรมการ

นายสมคิด จิรานันตรัตน์

อนุกรรมการ

ผู้แทนกระทรวงเกษตรและสหกรณ์
ผู้แทนกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ผู้แทนกระทรวงสาธารณสุข
ผู้แทนกรมการปกครอง
ผู้แทนกรมบัญชีกลาง
ผู้แทนกรมศุลกากร
ผู้แทนสำนักงานคณะกรรมการกฤษฎีกา
ผู้แทนสำนักงานคณะกรรมการข้าราชการพลเรือน
ผู้แทนสำนักงานคณะกรรมการพัฒนาระบบราชการ
ผู้แทนสำนักงบประมาณ
ผู้แทนสำนักงานการตรวจเงินแผ่นดิน
ผู้แทนธนาคารแห่งประเทศไทย
ผู้ทรงคุณวุฒิด้านสถาปัตยกรรมและมาตรฐานการพัฒนารัฐบาลดิจิทัล
- ผู้ช่วยศาสตราจารย์ภุชงค์ อุทโยภาศ
- นายพณชิต กิตติปัญญางาม
- นายศรัณย์ สัมฤทธิ์เดชขจร

อนุกรรมการและเลขานุการร่วม

ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ช่วยเลขานุการ

เจ้าหน้าที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

ประธานกรรมการ

ผู้ช่วยศาสตราจารย์ภุชงค์ อุทโยภาศ	มหาวิทยาลัยเกษตรศาสตร์

รองประธานกรรมการ

นายวิบูลย์ ภัทรพิบูล	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

กรรมการ

ผู้ช่วยศาสตราจารย์โษฑศ์รัตต ธรรมบุษดี	มหาวิทยาลัยมหิดล
ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย
นายสุทธิศักดิ์ ตันตะโยธิน	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
นายพณชิต กิตติปัญญางาม	สมาคมการค้าเพื่อส่งเสริมผู้ประกอบการเทคโนโลยีรายใหม่
นายมารุต บูรณรัช	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นางสาวปณิศา เหลืองวรเมท	สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ
นางสาวพลอย เจริญสม	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายศุภโชค จันทรประทิน	
นางบุญยิ่ง ชั่งสัจจา	สำนักบริหารการทะเบียน กรมการปกครอง
นายณัฏฐา พาชัยยุทธ	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นายพัชโรดม ลิมปิษเฐียร	สำนักงานคณะกรรมการกฤษฎีกา
นางสาวพัชรี ไชยเรืองกิตติ	
นางสาวสุภร สุขะตุงคะ	สำนักงานการตรวจเงินแผ่นดิน
นางสาวพลอยรวี เกริกพันธ์กุล	สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
นายทรงพล ใหม่สาลี	สำนักงานสถิติแห่งชาติ
นางกาญจนา ภู่มาลี	

กรรมการและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ

ที่ปรึกษา

นายสุพจน์ เธียรวุฒิ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ผู้ช่วยศาสตราจารย์ภุชงค์ อุทโยภาศ	มหาวิทยาลัยเกษตรศาสตร์

ประธานคณะทำงาน

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย

คณะทำงาน

นายเนติพงษ์ ตลับนาค	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ
นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายชาลี วรกุลพิพัฒน์	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
รองศาสตราจารย์เกริก ภิรมย์โสภา	จุฬาลงกรณ์มหาวิทยาลัย
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วิเคราะห์และจัดทำมาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม

นางสาวอัญชลี โพธิ์อ่อน	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นางสาวนงลักษณ์ พลอยสุภา	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายภัทร วานิชทวีวัฒน์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นางสาววีรวรรณ วระแสง	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม ฉบับนี้ สำหรับบุคคลธรรมดาและนิติบุคคล จัดทำขึ้นเพื่ออธิบายภาพรวมของการใช้งานดิจิทัลไอดีสำหรับบริการภาครัฐที่ครอบคลุมถึงบทนิยาม กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง แบบจำลองดิจิทัลไอดี ภาพรวมของการพิสูจน์และยืนยันตัวตนทางดิจิทัล กลุ่มการให้บริการภาครัฐ รวมถึงการบริหารจัดการความเสี่ยง เพื่อให้หน่วยงานที่เกี่ยวข้องกับการใช้ดิจิทัลไอดีมีความเข้าใจตรงกัน โดยพัฒนาตามแนวมาตรฐานของ NIST Special Publication 800-63-3 – Digital Identity Guidelines, National Institute of Standards and Technology, US Department of Commerce [๑] และข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ [๔] อีกทั้งได้มีการรับฟังความคิดเห็นจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้มาตรฐานรัฐบาลดิจิทัลฉบับนี้ มีความครบถ้วนสมบูรณ์ สามารถนำไปปรับใช้ในทางปฏิบัติได้

มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม ฉบับนี้ จัดทำขึ้นโดยคณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒คณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ ร่วมกับ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
อาคารบางกอกไทยทาวเวอร์ ๑๐๘ ถนนรางน้ำ
แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ ๑๐๔๐๐
โทรศัพท์: ๐ ๒๖๑๒ ๖๐๐๐
โทรสาร: ๐ ๒๖๑๒ ๖๐๑๑, ๐ ๒๖๑๒ ๖๐๑๒
E-mail: contact@dga.or.th
Website: www.dga.or.th

คำนำ

การจัดทำกระบวนการและการดำเนินงานทางดิจิทัลของภาครัฐ เป็นการวางรูปแบบร่วมกัน เพื่อสร้างขั้นตอนการทำงาน พัฒนาบริการให้เป็นรูปแบบดิจิทัลแบบครบวงจร สามารถเชื่อมโยงข้อมูลระหว่างหน่วยงานได้ โดยมีการนำระบบเทคโนโลยีดิจิทัลมาใช้ในการทำงาน เป็นกลไกในการเพิ่มประสิทธิภาพในการให้บริการภาครัฐแก่ประชาชน เป็นการเพิ่มทางเลือกให้แก่ประชาชนในการขอรับบริการจากภาครัฐ ช่วยลดความผิดพลาด ยกระดับการทำงานของภาครัฐผ่านระบบดิจิทัลตั้งแต่ต้นจนจบได้อย่างสมบูรณ์ นำไปสู่การเป็นรัฐบาลดิจิทัลที่ไร้กระดาษ (paperless) ซึ่งกระบวนการหลักของการดำเนินงานทางดิจิทัลของภาครัฐ เริ่มตั้งแต่การพิสูจน์และยืนยันตัวตนทางดิจิทัลไปจนถึงการจัดส่งใบอนุญาตหรือเอกสารต่าง ๆ ทางดิจิทัล

การพิสูจน์และยืนยันตัวตนทางดิจิทัล เป็นกระบวนการแรกที่สำคัญในการเข้าสู่บริการภาครัฐ ซึ่งหน่วยงานของรัฐต้องประเมินความต้องการของหน่วยงานเพื่อพิจารณาว่าบริการใดบ้างที่จำเป็นต้องใช้ดิจิทัลไอดีในการพิสูจน์และยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐ โดยมาตรฐานรัฐบาลดิจิทัลที่เกี่ยวข้องกับการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ 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)

สารบัญ

สารบัญตาราง

มาตรฐานรัฐบาลดิจิทัล

ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม

๑. ขอบข่าย

มาตรฐานรัฐบาลดิจิทัลฯ ฉบับนี้ เป็นแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม สำหรับบุคคลธรรมดาและนิติบุคคล ที่ครอบคลุมถึงบทนิยาม กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง แบบจำลองดิจิทัลไอดี ภาพรวมของการพิสูจน์และยืนยันตัวตนทางดิจิทัล กลุ่มการให้บริการภาครัฐ รวมถึงการบริหารจัดการความเสี่ยง เพื่อให้หน่วยงานที่เกี่ยวข้องกับการใช้ดิจิทัลไอดีมีความเข้าใจตรงกัน โดยอ้างอิงข้อกำหนด ดังนี้

(๑) มาตรฐาน NIST Special Publication 800-63-3 – Digital Identity Guidelines [๑]

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

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

(๔) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ [๔]

(๕) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน [๕]

(๖) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน [๖]

อย่างไรก็ตาม มาตรฐานรัฐบาลดิจิทัลฯ ฉบับนี้ จะเป็นคำแนะนำโดยทั่วไป ซึ่งไม่สามารถครอบคลุมประเด็นทางกฎหมายทั้งหมดที่อาจเกิดขึ้นได้ ดังนั้นหากมีข้อสงสัยเกี่ยวกับการดำเนินการตามเอกสารฉบับนี้หรือประเด็นอื่น ๆ ไม่ได้กล่าวถึงในที่นี้ ควรมีการปรึกษากับผู้เชี่ยวชาญทางกฎหมายตามความจำเป็น

๒. บทนิยาม

ความหมายของนิยามที่ใช้ในมาตรฐานรัฐบาลดิจิทัลฯ ฉบับนี้ มีดังนี้

๒.๑ บริการภาครัฐ หมายความว่า การดำเนินการอย่างหนึ่งอย่างใดที่หน่วยงานของรัฐจัดทำหรือจัดให้มีขึ้นหรือที่มอบอำนาจให้เอกชนดำเนินการแทน เพื่ออำนวยความสะดวกหรือตอบสนองความต้องการของประชาชน

๒.๒ ไอเดนทิตี (identity หรือ ID) หมายความว่า คุณลักษณะหรือชุดของคุณลักษณะที่ใช้ระบุตัวบุคคลในบริบทที่กำหนด [๔]

๒.๓ ดิจิทัลไอดี (digital Identity หรือ Digital ID) หมายความว่า คุณลักษณะหรือชุดของคุณลักษณะที่ถูกรวบรวมและบันทึกในรูปแบบดิจิทัล ซึ่งสามารถใช้ระบุตัวบุคคลในบริบทที่กำหนด และสามารถใช้ทำธุรกรรมอิเล็กทรอนิกส์ [๔]

๒.๔ ผู้พิสูจน์และยืนยันตัวตน (identity provider) หมายความว่า บุคคลหรือหน่วยงานที่น่าเชื่อถือซึ่งทำหน้าที่

(๑) รับลงทะเบียนและพิสูจน์ตัวตน และ
(๒) บริหารจัดการสิ่งที่ใช้รับรองตัวตน ซึ่งเชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ

โดยผู้พิสูจน์และยืนยันตัวตนอาจบริหารจัดการสิ่งที่ใช้รับรองตัวตน เพื่อใช้ภายในองค์กรหรือใช้ภายนอกองค์กรก็ได้

๒.๕ ผู้ให้บริการภาครัฐ (relying party) หมายความว่า หน่วยงานของรัฐที่ให้บริการภาครัฐหรืออนุญาตให้เข้าถึงข้อมูลหรือระบบบริการภาครัฐ โดยอาศัยสิ่งที่ใช้ยืนยันตัวตน และผลการยืนยันตัวตนหรือสิ่งที่ใช้รับรองตัวตนจากผู้พิสูจน์และยืนยันตัวตน

๒.๖ แหล่งให้ข้อมูลที่น่าเชื่อถือ (authoritative source) หมายความว่า หน่วยงานที่มีความน่าเชื่อถือและสามารถเข้าถึงหรือมีข้อมูลที่ถูกต้อง ซึ่งทำหน้าที่

(๑) ตรวจสอบข้อมูลหรือสถานะของหลักฐานแสดงตนของผู้ใช้บริการตามการร้องขอจากผู้พิสูจน์และยืนยันตัวตน หรือ
(๒) อนุญาตให้ผู้ให้บริการภาครัฐเข้าถึงข้อมูลที่น่าเชื่อถือหรือข้อมูลส่วนบุคคลซึ่งได้รับความยินยอมจากผู้ใช้บริการ

๒.๗ ผู้สมัครใช้บริการ (applicant) หมายความว่า บุคคลที่สมัครใช้บริการพิสูจน์และยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน

๒.๘ ผู้ใช้บริการ (subscriber) หมายความว่า ผู้สมัครใช้บริการที่ผ่านการลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตน และได้รับสิ่งที่ใช้ยืนยันตัวตนสำหรับใช้ยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน

๒.๙ การลงทะเบียน (enrolment) หมายความว่า กระบวนการที่ผู้สมัครใช้บริการลงทะเบียนเป็นผู้ใช้บริการของผู้พิสูจน์และยืนยันตัวตน [๔]

๒.๑๐ การพิสูจน์ตัวตน (identity proofing) หมายความว่า กระบวนการที่ผู้พิสูจน์และยืนยันตัวตนรวบรวมข้อมูล ตรวจสอบหลักฐานแสดงตน และตรวจสอบตัวตนของผู้สมัครใช้บริการ [๔]

๒.๑๑ การยืนยันตัวตน (authentication) หมายความว่า กระบวนการที่ผู้ใช้บริการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตนว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างด้วยการใช้สิ่งที่ใช้ยืนยันตัวตน [๔]

๒.๑๒ สิ่งที่ใช้ยืนยันตัวตน (authenticator) หมายความว่า สิ่งที่ผู้ใช้บริการครอบครองเพื่อใช้ในการยืนยันตัวตน โดยสิ่งที่ใช้ยืนยันตัวตนจะมีปัจจัยของการยืนยันตัวตนอย่างน้อยหนึ่งปัจจัย [๔]

๒.๑๓ สิ่งที่ใช้รับรองตัวตน (credential) หมายความว่า เอกสาร วัตถุ หรือกลุ่มข้อมูล ที่เชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตน [๔]

๒.๑๔ คุณลักษณะ (attribute) หมายความว่า ลักษณะหรือคุณสมบัติของบุคคล [๔]

๒.๑๕ แหล่งออกหลักฐานแสดงตน (issuing source) หมายความว่า หน่วยงานที่รับผิดชอบในการจัดทำข้อมูลหลักฐานทางดิจิทัลหรือเอกสารที่ใช้เป็นหลักฐานแสดงตน

๓. กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง

การใช้ดิจิทัลไอดีสำหรับบริการภาครัฐมีการบัญญัติไว้ในกฎหมายหรือแนวปฏิบัติที่เกี่ยวข้อง ดังนี้

๓.๑ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๔) พ.ศ. ๒๕๖๒ กำหนดให้มีการกำกับดูแลการพิสูจน์และยืนยันตัวตนทางดิจิทัลให้มีความน่าเชื่อถือและปลอดภัย ซึ่งจะเป็นประโยชน์ต่อเศรษฐกิจของประเทศและการคุ้มครองผู้บริโภค

๓.๒ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ในมาตรา ๑๒ (๔) กำหนดให้หน่วยงานของรัฐจัดให้มีระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อประโยชน์ในการอำนวยความสะดวกของการให้บริการประชาชน ซึ่งมีมาตรฐานและแนวทางที่สอดคล้องกันตามที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด

๓.๓ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้มีการกำหนดหลักเกณฑ์ กลไก และมาตรการที่กำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล

๓.๔ ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย ดังนี้

๓.๔.๑ ภาพรวมและอภิธานศัพท์ (ขมธอ. ๑๘-๒๕๖๑) เป็นการอธิบายภาพรวมและอภิธานศัพท์เกี่ยวกับการใช้งานดิจิทัลไอดีสำหรับประเทศไทย การบริหารความเสี่ยง และการกำหนดระดับความน่าเชื่อถือ

๓.๔.๒ การลงทะเบียนและพิสูจน์ตัวตน (ขมธอ. ๑๙-๒๕๖๑) เป็นการอธิบายข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน ในการลงทะเบียนและพิสูจน์ตัวตนของผู้สมัครใช้บริการที่ประสงค์จะทำธุรกรรมออนไลน์ด้วยดิจิทัลไอดี ตามระดับความน่าเชื่อถือของไอเดนทิตี

๓.๔.๓ การยืนยันตัวตน (ขมธอ. ๒๐-๒๕๖๑) เป็นการอธิบายข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน ในการยืนยันตัวตนของผู้ใช้บริการที่ประสงค์จะทำธุรกรรมออนไลน์ด้วยดิจิทัลไอดี ตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

๔. แบบจำลองดิจิทัลไอดี (Digital Identity Model)

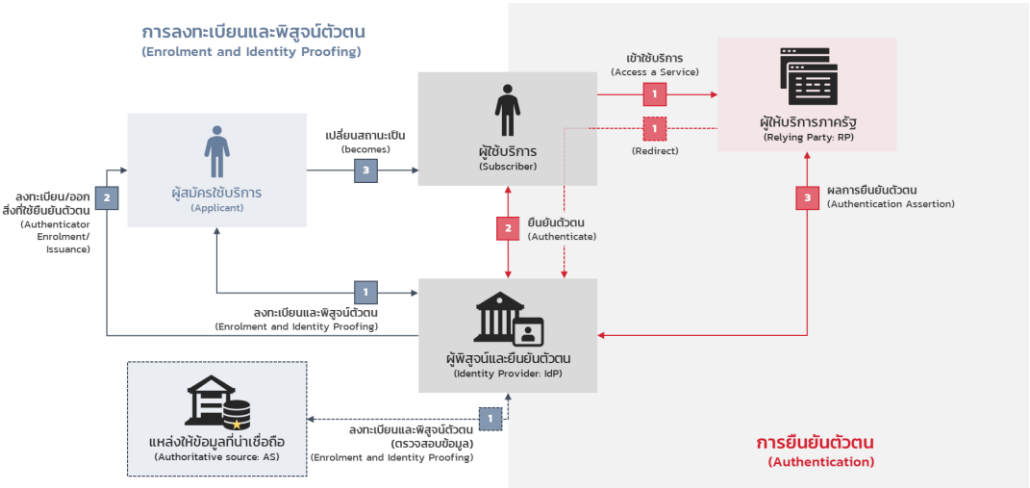
๔.๑ ภาพรวม (Overview)

ดิจิทัลไอดี (digital identity) คือ คุณลักษณะเฉพาะสำหรับเข้าใช้บริการธุรกรรมออนไลน์ของภาครัฐ ซึ่งเป็นกระบวนการที่ประกอบด้วย การลงทะเบียนและพิสูจน์ตัวตน (enrolment and identity proofing) และการยืนยันตัวตน (authentication) โดยผู้ถูกพิสูจน์ตัวตนจะเรียกว่า “ผู้สมัครใช้บริการ (applicant)” และเมื่อผู้สมัครใช้บริการทำการพิสูจน์ตัวตนแล้วว่าเป็นบุคคลนั้นจริง หรือเป็นเจ้าของไอเดนทิตีนั้นจริงจะถูกเปลี่ยนสถานะเป็น “ผู้ใช้บริการ (subscriber)”

ในการวัดระดับความเข้มงวดของกระบวนการพิสูจน์ตัวตน เรียกว่า “ระดับความน่าเชื่อถือของไอเดนทิตี (identity assurance level: IAL)” ประกอบด้วย IAL1 IAL2 และ IAL3 โดย IAL1 IAL2 และ IAL3 จะมีข้อกำหนดในการพิสูจน์ตัวตนจำแนกตามกลุ่มการให้บริการภาครัฐในรูปแบบดิจิทัล (รายละเอียดจะกล่าวต่อไปในมาตรฐานรัฐบาลดิจิทัลฯ เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล)

ผู้ใช้บริการเข้าใช้บริการของผู้ให้บริการภาครัฐ (relying party: RP) จะต้องยืนยันตัวตนว่าเป็นบุคคลนั้นจริง หรือเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างนั้นจริง โดยแสดงให้ผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) เห็นว่าตนครอบครองสิ่งที่ใช้ยืนยันตัวตนตามเกณฑ์ที่กำหนด เมื่อผู้พิสูจน์และยืนยันตัวตนตรวจสอบความถูกต้องจะส่งผลการยืนยันตัวตนให้กับผู้ให้บริการภาครัฐ โดยผู้ให้บริการภาครัฐสามารถใช้ข้อมูลที่อยู่ในผลการยืนยันตัวตนไปพิจารณาสิทธิ ทั้งนี้ต้องมีกระบวนการที่ผู้ใช้บริการอนุญาตให้ผู้ให้บริการภาครัฐเข้าถึงข้อมูลของตน (authorization)

ในการวัดระดับความเข้มงวดของกระบวนการยืนยันตัวตน เรียกว่า “ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (authenticator assurance level: AAL)” ประกอบด้วย AAL1 AAL2 และ AAL3 โดย AAL1 ต้องใช้การยืนยันตัวตนแบบปัจจัยเดียว (single-factor authentication) ในขณะที่ AAL2 ต้องใช้การยืนยันตัวตนแบบ ๒ ปัจจัยที่แตกต่างกัน (two-factor authentication: 2FA) และ AAL3 ต้องใช้การยืนยันตัวตนเช่นเดียวกับ AAL2 แต่ควรมีหนึ่งปัจจัยที่เป็นอุปกรณ์ที่ใช้ในการยืนยันตัวตน (hardware-base) และต้องป้องกันการปลอมแปลงเป็นบุคคลอื่นได้



รูปที่ ๑ ภาพรวมวงจรชีวิตของการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ที่มา: ปรับปรุงจาก (NIST, NIST Special Publication 800-63-3 – Digital Identity Guidelines, 2017) [๑]

จากรูปที่ ๑ แสดงให้เห็นว่าการพิสูจน์และยืนยันตัวตนทางดิจิทัล มีทั้งหมด ๒ กระบวนการหลัก ได้แก่ (๑) การลงทะเบียนและพิสูจน์ตัวตน (๒) การยืนยันตัวตน ทั้งนี้ ผู้พิสูจน์และยืนยันตัวตน ต้องมีส่วนร่วมในการบริหารจัดการระบบให้มีความต่อเนื่องและมั่นคงปลอดภัย เช่น การเพิ่ม ปรับปรุง หรือยกเลิกข้อมูลไอเดนทิตีของผู้สมัครใช้บริการและผู้ใช้บริการให้เป็นปัจจุบัน

จากรูปที่ ๑ ด้านซ้าย เป็นกระบวนการลงทะเบียนและพิสูจน์ตัวตน ซึ่งมีขั้นตอน ดังนี้

(๑) ผู้สมัครใช้บริการลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตน โดยผู้พิสูจน์และยืนยันตัวตนอาจตรวจสอบข้อมูลกับแหล่งให้ข้อมูลที่น่าเชื่อถือ

(๒) หากพิสูจน์ตัวตนสำเร็จ ผู้พิสูจน์และยืนยันตัวตนจะลงทะเบียนหรือออกสิ่งที่ใช้ยืนยันตัวตน และสร้างสิ่งที่ใช้รับรองตัวตนให้กับผู้ใช้บริการ

(๓) ผู้สมัครใช้บริการ เปลี่ยนสถานะเป็น ผู้ใช้บริการ

หมายเหตุ *ผู้พิสูจน์และยืนยันตัวตน ต้องเก็บรักษาสิ่งที่ใช้รับรองตัวตน สถานะของสิ่งที่ใช้รับรองตัวตน และข้อมูลที่ใช้ในกระบวนการลงทะเบียน ตลอดอายุการใช้งานของสิ่งที่ใช้รับรองตัวตน (เป็นอย่างน้อย) ส่วนผู้ใช้บริการต้องเก็บรักษาสิ่งที่ใช้ยืนยันตัวตน*

จากรูปที่ ๑ ด้านขวา เป็นกระบวนการยืนยันตัวตน ซึ่งมีขั้นตอน ดังนี้

(๑) ผู้ใช้บริการขอเข้าใช้บริการกับผู้ให้บริการภาครัฐ โดยผู้ให้บริการภาครัฐอาจให้ผู้ใช้บริการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตนแทน (redirect)

(๒) ผู้พิสูจน์และยืนยันตัวตนต้องตรวจสอบสิ่งที่ใช้ยืนยันตัวตนที่เชื่อมโยงไอเดนทิตีของผู้ใช้บริการ

๔.๒ การลงทะเบียนและพิสูจน์ตัวตน (Enrolment and Identity Proofing)

๔.๒.๑ การลงทะเบียน (Enrolment)

เป็นกระบวนการได้มาและการบันทึกข้อมูลไอเดนทิตีที่จำเป็นจากผู้สมัครใช้บริการ ซึ่งอ้างอิงมาจากข้อมูลประวัติ เช่น ชื่อ ชื่อสกุล วันเดือนปีเกิด เพศ ที่อยู่ อีเมล และได้จากข้อมูลชีวมิติ (biometric) เช่น ลายนิ้วมือ รูม่านตา รวมถึงการนำคุณลักษณะอื่น ๆ เพิ่มเติมประกอบเข้าด้วยกัน สำหรับบัตรประจำตัวประชาชนจะต้องได้ข้อมูลอย่างน้อย เช่น เลขประจำตัวประชาชน ชื่อ ชื่อสกุล วันเดือนปีเกิด เลขหลังบัตรประจำตัวประชาชน (laser code) โดยคุณลักษณะดังกล่าวจะต้องแสดงให้เห็นว่าไอเดนทิตีที่ได้มามีความน่าเชื่อถือ มีเพียงหนึ่งเดียว และมีความเฉพาะเจาะจงภายในบริบทของผู้ใช้บริการทั้งหมดที่ผู้พิสูจน์และยืนยันตัวตนดูแล

๔.๒.๒ การพิสูจน์ตัวตน (Identity Proofing)

เป็นกระบวนการตรวจสอบหลักฐานแสดงตนและตรวจสอบตัวบุคคล เมื่อมีผู้สมัครใช้บริการอ้างความเป็นเจ้าของไอเดนทิตีในระหว่างการลงทะเบียนนั้น ทำให้ไอเดนทิตีถูกตรวจสอบโดยเปรียบเทียบกับคุณลักษณะของข้อมูลที่มีอยู่ ดังนั้นกระบวนการพิสูจน์ตัวตนดังกล่าวทำให้มั่นใจได้ว่าไอเดนทิตีนั้นมีอยู่จริง เช่น การตรวจสอบเพื่อยืนยันว่าผู้สมัครใช้บริการเป็นบุคคลนั้นจริงและมีเพียงหนึ่งเดียว โดยอาจตรวจสอบไอเดนทิตีที่กล่าวอ้างกับไอเดนทิตีบนฐานข้อมูลแห่งอื่น เช่น ระบบทะเบียนราษฎร์ หลังจากนั้นผู้พิสูจน์และยืนยันตัวตน

จะออกสิ่งที่ใช้รับรองตัวตนในรูปแบบดิจิทัล เพื่อใช้ในกระบวนการยืนยันตัวตน เช่น บัตรประจำตัวประชาชน หนังสือเดินทาง ใบรับรองอิเล็กทรอนิกส์

๔.๒.๓ วิธีการพิสูจน์ตัวตน (Identity Proofing Methods)

อ้างอิงจากประกาศธนาคารแห่งประเทศไทย ที่ สนส. ๑๙/๒๕๖๒ เรื่อง หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน [๙] และข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทำธุรกรรมแบบพบเห็นลูกค้าต่อหน้าสำหรับธนาคาร [๑๐] โดยทั่วไปแล้วมีรูปแบบของการแสดงตนเพื่อพิสูจน์ตัวตน ๓ รูปแบบ ได้แก่ (๑) พบเห็นต่อหน้า (๒) ไม่พบเห็นต่อหน้า และ (๓) เสมือนพบเห็นต่อหน้า

๔.๒.๓.๑ พบเห็นต่อหน้า (Face-to-Face)

ผู้สมัครใช้บริการต้องแสดงตนพร้อมนำข้อมูลและหลักฐานแสดงตนยื่นต่อหน้าเจ้าหน้าที่ที่มีหน้าที่รับผิดชอบและผ่านการฝึกอบรมที่ผู้พิสูจน์และยืนยันตัวตนกำหนดให้เป็นผู้ตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบันของข้อมูล เพื่อพิสูจน์ว่าเป็นบุคคลนั้นจริงและมีเพียงหนึ่งเดียว

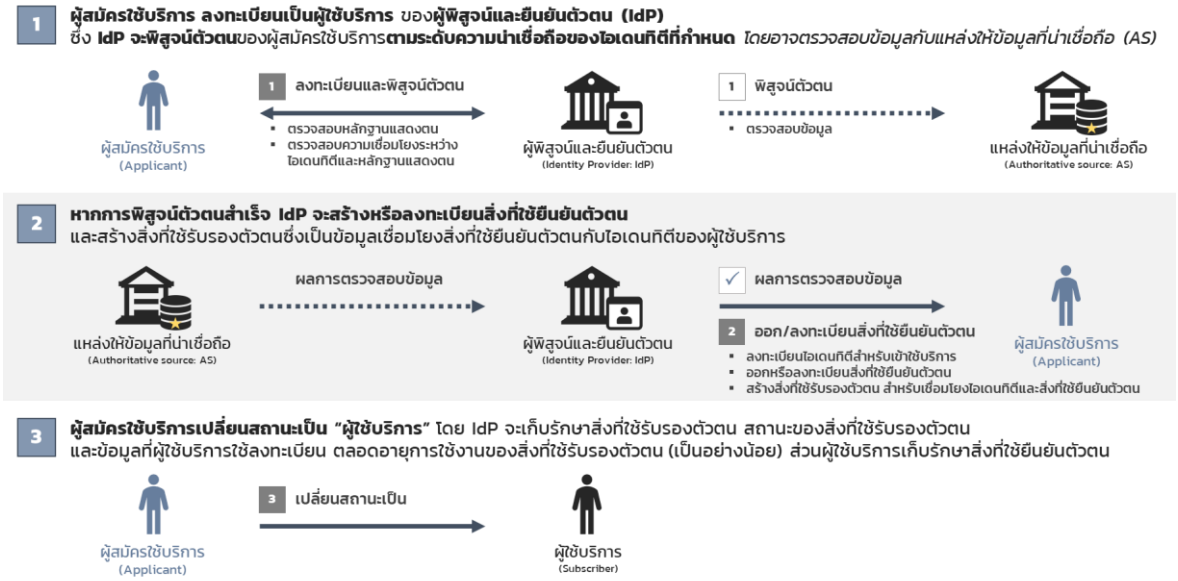
๔.๒.๓.๒ ไม่พบเห็นต่อหน้า (Non Face-to-Face)

ผู้พิสูจน์และยืนยันตัวตนต้องจัดให้มีกระบวนการลงทะเบียนและพิสูจน์ตัวตนผ่านระบบดิจิทัลที่มีความน่าเชื่อถือ และมีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยในการตรวจสอบข้อมูลและหลักฐานแสดงตนของผู้สมัครใช้บริการเทียบเท่ากับการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า หรือเสมือนพบเห็นต่อหน้า เช่น การใช้เทคโนโลยีเพื่อพิสูจน์ความเป็นบุคคลและสังเกตพฤติกรรมผู้สมัครใช้บริการ (liveness detection) และเทคโนโลยีเปรียบเทียบข้อมูลชีวมิติของผู้สมัครใช้บริการ (biometric comparison) เพื่อพิสูจน์ว่าเป็นผู้สมัครใช้บริการรายนั้นจริง ทดแทนการพบเห็นต่อหน้า ถ้าไม่สามารถสังเกตพฤติกรรมของผู้สมัครใช้บริการ ผู้พิสูจน์และยืนยันตัวตนต้องกำหนดกระบวนการหรือแนวทางการบริหารความเสี่ยงเพิ่มเติมเพื่อลดความเสี่ยงจากกรณีทุจริตต่าง ๆ ได้

๔.๒.๓.๓ เสมือนพบเห็นต่อหน้า (Supervised Remote)

ผู้พิสูจน์และยืนยันตัวตนต้องจัดให้มีกระบวนการลงทะเบียนและพิสูจน์ตัวตนผ่านระบบดิจิทัลที่มีความน่าเชื่อถือ และมีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยในการตรวจสอบข้อมูลและหลักฐานแสดงตนของผู้สมัครใช้บริการเทียบเท่ากับการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า รวมถึงจัดให้มีเจ้าหน้าที่ที่มีหน้าที่รับผิดชอบและผ่านการฝึกอบรม ทำหน้าที่เฝ้าสังเกตและเข้าร่วมสนทนาออนไลน์กับผู้สมัครใช้บริการแบบถ่ายทอดสดตลอดเวลาของการลงทะเบียนและพิสูจน์ตัวตน เช่น การส่งผ่านวิดีโอที่มีความละเอียดสูงอย่างต่อเนื่อง (high resolution video transmission)

๔.๒.๔ กระบวนการลงทะเบียนและพิสูจน์ตัวตน (Enrolment and Identity Proofing Process)



รูปที่ ๒ กระบวนการลงทะเบียนและพิสูจน์ตัวตน

ที่มา: ปรับปรุงจาก (ขมธอ. ๑๘-๒๕๖๑ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์) [๔]

จากรูปที่ ๒ ประกอบด้วย ๓ กระบวนการ ดังนี้

(๑) ผู้สมัครใช้บริการลงทะเบียนกับผู้พิสูจน์และยืนยันตัวตนที่ตนต้องการใช้บริการพิสูจน์และยืนยันตัวตน ซึ่งผู้พิสูจน์และยืนยันตัวตนจะดำเนินการพิสูจน์ตัวตนของผู้สมัครใช้บริการ โดยรวบรวมข้อมูลเพื่อระบุตัวตน ตรวจสอบหลักฐานแสดงตน และตรวจสอบตัวบุคคลตามระดับความน่าเชื่อถือของไอเดนทิตีที่กำหนด ทั้งนี้ อาจตรวจสอบข้อมูลกับแหล่งให้ข้อมูลที่น่าเชื่อถือ

(๒) หากการพิสูจน์ตัวตนสำเร็จ ผู้พิสูจน์และยืนยันตัวตนจะดำเนินการ ดังนี้

(๒.๑) ลงทะเบียนไอเดนทิตีที่ใช้ระบุตัวตนผู้ใช้บริการแต่ละราย เช่น สร้างเลขประจำตัวให้กับผู้ใช้บริการหรือลงทะเบียนชื่อผู้ใช้บริการ (user ID) ที่ไม่ซ้ำกัน

(๒.๒) ออกหรือลงทะเบียนสิ่งที่ใช้ยืนยันตัวตนให้กับผู้ใช้บริการ โดยชนิดของสิ่งที่ใช้ยืนยันตัวตนขึ้นอยู่กับระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

(๒.๓) สร้างสิ่งที่ใช้รับรองตัวตนซึ่งเป็นข้อมูลเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตีของผู้ใช้บริการ เพื่อให้ผู้ใช้บริการสามารถนำสิ่งที่ใช้ยืนยันตัวตนดังกล่าวมาใช้ยืนยันตัวตนในอนาคต

(๓) ผู้สมัครใช้บริการเปลี่ยนสถานะเป็น “ผู้ใช้บริการ” โดยผู้พิสูจน์และยืนยันตัวตนจะเก็บรักษาสิ่งที่ใช้รับรองตัวตน สถานะของสิ่งที่ใช้รับรองตัวตน และข้อมูลที่ผู้ใช้บริการใช้ลงทะเบียนตลอดอายุการใช้งานของสิ่งที่ใช้รับรองตัวตน (เป็นอย่างน้อย) ส่วนผู้ใช้บริการเก็บรักษาสิ่งที่ใช้ยืนยันตัวตน

๔.๓ การยืนยันตัวตน (Authentication)

๔.๓.๑ สิ่งที่ใช้ยืนยันตัวตน (Authenticators)

สิ่งที่ใช้ยืนยันตัวตน คือ สิ่งที่ผู้ใช้บริการครอบครองและใช้ในการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตนว่าเป็นบุคคลที่กล่าวอ้างจริง สิ่งที่ใช้ยืนยันตัวตนอาจประกอบด้วยปัจจัยของการยืนยันตัวตนเพียงหนึ่งปัจจัยหรือมากกว่าหนึ่งปัจจัยก็ได้ อย่างไรก็ตาม ความปลอดภัยของระบบยืนยันตัวตน (authentication system) ขึ้นอยู่กับความสามารถในการป้องกันการโจมตีของสิ่งที่ใช้ยืนยันตัวตนและจำนวนปัจจัยของการยืนยันตัวตน โดยปัจจัยของการยืนยันตัวตน (authentication factor) แบ่งออกเป็น ๓ ประเภท ดังนี้

(๑) สิ่งที่ผู้ใช้บริการรู้ (something you know) คือ ข้อมูลที่ผู้ใช้บริการเท่านั้นที่ทราบ เช่น รหัสผ่าน

(๒) สิ่งที่ผู้ใช้บริการมี (something you have) คือ สิ่งที่ผู้ใช้บริการเท่านั้นที่ครอบครอง เช่น บัตรประจำตัวประชาชน

(๓) สิ่งที่ผู้ใช้บริการเป็น (something you are) คือ ข้อมูลทางชีวมิติของผู้ใช้บริการเท่านั้น เช่น ลายนิ้วมือ ใบหน้า

ข้อมูลลับ (secrets) คือ สิ่งที่ใช้ยืนยันตัวตนจะมีข้อมูลลับที่เฉพาะผู้ใช้บริการตัวจริงเท่านั้นครอบครอง ข้อมูลลับที่อยู่ในสิ่งที่ใช้ยืนยันตัวตนเป็นได้ทั้งกุญแจแบบอสมมาตร (การเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสคนละตัว) หรือกุญแจแบบสมมาตร (การเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสตัวเดียวกัน) ในกรณีกุญแจแบบอสมมาตร คือใช้กุญแจสาธารณะ (public key) และกุญแจส่วนตัว (private key) ซึ่งผู้ใช้บริการจะใช้กุญแจส่วนตัวที่อยู่ในสิ่งที่ใช้ยืนยันตัวตนเพื่อยืนยันตัวตน โดยผู้พิสูจน์และยืนยันตัวตนจะใช้กุญแจสาธารณะกับกุญแจส่วนตัวของผู้ที่กล่าวอ้างมาจับคู่กัน (key pairs) เพื่อพิสูจน์ความเป็นเจ้าของและครอบครองสิ่งที่ใช้ยืนยันตัวตนนั้นจริง อนึ่ง ข้อมูลลับที่ใช้รหัสตัวเดียวกัน (shared secret) ที่อยู่ในสิ่งที่ใช้ยืนยันตัวตนอาจเป็นได้ทั้งกุญแจแบบสมมาตร หรือรหัสลับจดจำ (memorized secret) โดยข้อแตกต่างระหว่างกุญแจแบบสมมาตรและรหัสลับจดจำ คือ กุญแจแบบสมมาตรมักสร้างจากระบบสุ่มและเก็บไว้ในอุปกรณ์ฮาร์ดแวร์หรือซอฟต์แวร์ ในขณะที่รหัสลับจดจำเป็นข้อมูลที่ผู้ใช้บริการสามารถจดจำได้

การยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) สามารถทำได้ ๒ รูปแบบ ดังนี้

(๑) ใช้ปัจจัยของการยืนยันตัวตนมากกว่าหนึ่งปัจจัยแสดงต่อผู้พิสูจน์และยืนยันตัวตนโดยตรง เช่น ผู้ใช้บริการต้องใช้รหัสผ่าน (สิ่งที่ผู้ใช้บริการรู้) และรหัสผ่านแบบใช้ครั้งเดียวที่ได้รับทางโทรศัพท์เคลื่อนที่ (สิ่งที่ผู้ใช้บริการมี) เพื่อยืนยันตัวตน

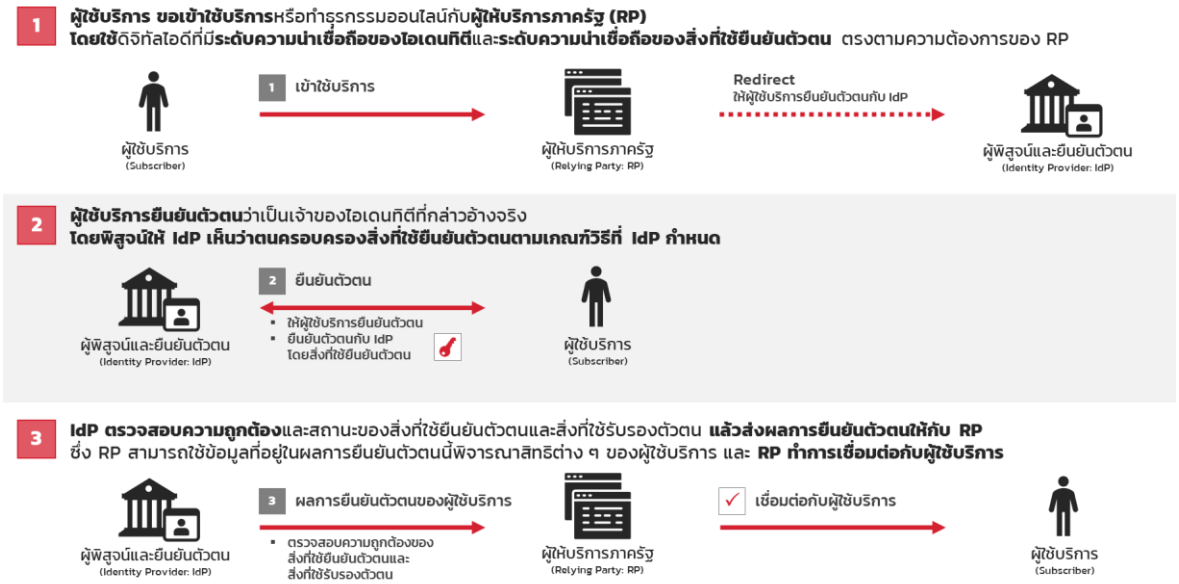
(๒) มีอย่างน้อยหนึ่งปัจจัยที่ปกป้องข้อมูลลับซึ่งเป็นอีกปัจจัยหนึ่ง เช่น ใช้อุปกรณ์ฮาร์ดแวร์ที่มีวิธีการเข้ารหัสลับ (สิ่งที่ผู้ใช้บริการมี) และใช้ลายนิ้วมือ (สิ่งที่ผู้ใช้บริการเป็น) ในการเข้าถึงอุปกรณ์ดังกล่าวนั้น เพื่อยืนยันตัวตน

ทั้งนี้ หากชนิดของสิ่งที่ใช้ยืนยันตัวตนเป็นอุปกรณ์เข้ารหัสลับ (cryptographic device) ต้องเป็นไปตามมาตรฐาน FIPS 140-2 (Federal Information Processing Standard Publication 140-2) ตามระดับที่เหมาะสม หรือมาตรฐานอื่นที่เทียบเท่า

๔.๓.๒ สิ่งที่ใช้รับรองตัวตน (Credentials)

สิ่งที่ใช้รับรองตัวตน คือ เอกสาร วัตถุ หรือกลุ่มข้อมูลที่เชื่อมโยงไอเดนทิตีของผู้ใช้บริการเข้ากับสิ่งที่ใช้ยืนยันตัวตน ซึ่งสิ่งที่ใช้รับรองตัวตนจะถูกเก็บและดูแลโดยผู้พิสูจน์และยืนยันตัวตน เช่น ฐานข้อมูลที่เชื่อมโยงไอเดนทิตีของผู้ใช้บริการเข้ากับสิ่งที่ใช้ยืนยันตัวตน ในขณะที่ผู้ใช้บริการจะครอบครองสิ่งที่ใช้ยืนยันตัวตน เช่น กุญแจส่วนตัว PIN รหัสผ่าน แต่ไม่จำเป็นต้องครอบครองสิ่งที่ใช้รับรองตัวตน

๔.๓.๓ กระบวนการยืนยันตัวตน (Authentication Process)



รูปที่ ๓ กระบวนการยืนยันตัวตน

ที่มา: ปรับปรุงจาก (ขมธอ. ๑๘-๒๕๖๑ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์) [๔]

จากรูปที่ ๓ เมื่อผู้สมัครใช้บริการลงทะเบียนและพิสูจน์ตัวตนสำเร็จ และถูกปรับสถานะเป็นผู้ใช้บริการเรียบร้อยแล้ว ในกรณีที่ต้องการเข้าใช้บริการภาครัฐของผู้ให้บริการภาครัฐ จะมีกระบวนการ ๓ กระบวนการ ดังนี้

(๑) ผู้ใช้บริการขอเข้าใช้บริการ และผู้ให้บริการภาครัฐต้องการทราบว่าผู้ใช้บริการเป็นผู้ใด สำหรับผู้ใช้บริการที่เคยลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตนที่ผู้ให้บริการภาครัฐเชื่อถือ ผู้ให้บริการภาครัฐจะนำผู้ใช้บริการ (redirect) ไปยังหน้าต่างยืนยันตัวตนของผู้พิสูจน์และยืนยันตัวตนนั้น

(๒) ผู้ใช้บริการต้องยืนยันตัวตนด้วยการแสดงสิ่งที่ใช้ยืนยันตัวตนต่อผู้พิสูจน์และยืนยันตัวตน โดยพิสูจน์ให้เห็นว่าตนครอบครองสิ่งที่ใช้ยืนยันตัวตนตามเกณฑ์วิธีที่ผู้พิสูจน์และยืนยันตัวตนกำหนด

(๓) เมื่อผู้พิสูจน์และยืนยันตัวตนตรวจสอบสิ่งที่ใช้ยืนยันตัวตนและสิ่งที่ใช้รับรองตัวตนเรียบร้อยแล้ว ผู้พิสูจน์และยืนยันตัวตนจะส่งผลการยืนยันตัวตนให้กับผู้ให้บริการภาครัฐ เพื่อให้ผู้ให้บริการภาครัฐนำไปใช้พิจารณาอนุญาตเข้าใช้บริการภาครัฐ หรือให้เข้าถึงข้อมูลหรือระบบต่อไป

๕. การจำแนกกลุ่มการให้บริการภาครัฐในรูปแบบดิจิทัล (Government Digital Service Classification)

เนื่องด้วยการให้บริการภาครัฐมีรูปแบบที่หลากหลาย เพื่อให้เกิดความชัดเจนในการให้บริการ จึงจำแนกกลุ่มการให้บริการภาครัฐในรูปแบบดิจิทัลออกเป็น ๔ กลุ่ม [๘] ดังนี้

๕.๑ กลุ่มการให้บริการข้อมูลพื้นฐาน (Emerging Services)

เป็นการให้บริการเผยแพร่ข้อมูลข่าวสารทั่วไปของหน่วยงานของรัฐ เช่น นโยบายสาธารณะ การกำกับดูแล กฎหมาย ระเบียบ เอกสารที่เกี่ยวข้อง และประเภทการให้บริการภาครัฐ ผ่านทางเว็บไซต์หรือช่องทางให้บริการข้อมูลข่าวสารอื่น โดยมีแนวทางการพิจารณา อย่างน้อยดังนี้

(๑) เป็นข้อมูลเปิดสาธารณะหรือข้อมูลทั่วไป

(๒) ไม่จำเป็นต้องใช้ข้อมูลส่วนบุคคล

(๓) ไม่จำเป็นต้องมีการลงทะเบียนและพิสูจน์ตัวตน

๕.๒ กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ (Enhanced Services)

เป็นการให้บริการข้อมูลข่าวสารของหน่วยงานของรัฐในรูปแบบการสื่อสารทางเดียวหรือสองทางกับผู้ใช้บริการ เช่น การรับแจ้งเรื่องร้องเรียน ข้อเสนอแนะ หรือแสดงความคิดเห็น ผ่านทางเว็บไซต์หรือช่องทางให้บริการข้อมูลข่าวสารอื่น โดยมีแนวทางการพิจารณา อย่างน้อยดังนี้

(๑) มีการสื่อสารโต้ตอบกับผู้ใช้บริการ

(๒) ใช้ข้อมูลส่วนบุคคลหรือไม่ก็ได้ โดยเจ้าของข้อมูลส่วนบุคคลไม่จำเป็นต้องเป็นผู้ดำเนินการเอง

(๓) มีการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลหรือไม่ก็ได้

(๔) มีช่องทางที่สามารถติดต่อได้

๕.๓ กลุ่มการให้บริการธุรกรรม (Transactional Services)

เป็นการให้บริการธุรกรรมของหน่วยงานของรัฐซึ่งมีผลผูกพันทางกฎหมาย เช่น การอนุญาต การจดทะเบียน หรือการดำเนินการใด ๆ กับหน่วยงานของรัฐ โดยมีแนวทางการพิจารณาอย่างน้อยดังนี้

(๑) ใช้ข้อมูลส่วนบุคคล เช่น เลขประจำตัวประชาชน ๑๓ หลัก โดยเจ้าของข้อมูลส่วนบุคคลเป็นผู้ดำเนินการเอง ณ ขณะนั้น

(๒) มีการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล

(๓) ยืนยันช่องทางการติดต่อ เช่น หมายเลขโทรศัพท์เคลื่อนที่ หรืออีเมล

๕.๔ กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงานที่มีความเสี่ยงสูง (Connected Services)

เป็นการให้บริการธุรกรรมที่มีการเชื่อมโยงข้อมูลระหว่างหน่วยงานที่มีความเสี่ยงสูง และมีผลผูกพันทางกฎหมาย เช่น การขอรับบริการภาครัฐแบบเบ็ดเสร็จ ณ จุดเดียว โดยมีแนวทางการพิจารณาอย่างน้อยดังนี้

(๑) มีการเชื่อมโยงหรือใช้ข้อมูลร่วมกับหน่วยงานภายนอกแห่งอื่น ซึ่งเป็นธุรกรรมที่มีความเสี่ยงสูง

(๒) ใช้ข้อมูลส่วนบุคคล เช่น เลขประจำตัวประชาชน ๑๓ หลัก โดยเจ้าของข้อมูลส่วนบุคคลเป็นผู้ดำเนินการเอง ณ ขณะนั้น หรือมีการมอบอำนาจ

(๓) การลงทะเบียนและพิสูจน์ตัวตนครั้งแรก ต้องมีการพบเห็นต่อหน้า หรือเสมือนพบเห็นต่อหน้าโดยดำเนินการต่อหน้าเจ้าหน้าที่ที่มีหน้าที่รับผิดชอบและผ่านการอบรม

(๔) ยืนยันช่องทางการติดต่อ เช่น หมายเลขโทรศัพท์เคลื่อนที่ หรืออีเมล

๖. การบริหารความเสี่ยงของดิจิทัลไอดี (Digital Identity Risk Management)

๖.๑ ภาพรวม (Overview)

ความเสี่ยงของการใช้ดิจิทัลไอดีตามมาตรฐานรัฐบาลดิจิทัลฯ ฉบับนี้ แบ่งออกเป็น ๒ ด้าน ดังนี้

(๑) การพิสูจน์ตัวตนผิดพลาด เช่น ผู้สมัครใช้บริการแอบอ้างไอเดนทิตีของบุคคลอื่นในการลงทะเบียน

(๒) การยืนยันตัวตนผิดพลาด เช่น ผู้ที่กล่าวอ้างใช้สิ่งที่ใช้ยืนยันตัวตนที่ไม่ใช่ของตนในการเข้าใช้บริการภาครัฐ

การประเมินความเสี่ยงในกระบวนการพิสูจน์และยืนยันตัวตน เพื่อช่วยให้สามารถเลือกใช้เทคโนโลยีหรือกลยุทธ์ที่เหมาะสมในการบรรเทาความเสี่ยงที่อาจเกิดขึ้น โดยวิธีการสำคัญในการประเมินความเสี่ยงดังกล่าว คือ การใช้วิธีการพิสูจน์ตัวตนและวิธีการยืนยันตัวตนที่มีความเข้มงวดสอดคล้องกับระดับผลกระทบและโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น

๖.๒ ระดับความน่าเชื่อถือ (Assurance Levels)

ผู้ให้บริการภาครัฐต้องกำหนดระดับความน่าเชื่อถือของแต่ละบริการตามผลการประเมินความเสี่ยง ซึ่งแบ่งระดับความน่าเชื่อถือออกเป็น ๒ ด้าน ดังนี้

๖.๒.๑ ระดับความน่าเชื่อถือของไอเดนทิตี (Identity Assurance Level: IAL)

ระดับความน่าเชื่อถือของไอเดนทิตี คือ ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของผู้สมัครใช้บริการ ซึ่งการกำหนดระดับความน่าเชื่อถือของไอเดนทิตีที่เหมาะสมจะช่วยลดโอกาสของการพิสูจน์ตัวตนผิดพลาด โดยระดับความน่าเชื่อถือของไอเดนทิตี แบ่งออกเป็น ๓ ระดับ ดังนี้

(๑) ระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๑ (IAL1)

มีการรวบรวมข้อมูลเพื่อระบุตัวตน เพื่อพิจารณาและตรวจสอบหลักฐานแสดงตนหรือไม่ก็ได้ ทั้งนี้ ไม่มีข้อกำหนดในการแสดงตนและตรวจสอบตัวบุคคลโดยผู้พิสูจน์และยืนยันตัวตน เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงต่ำ

(๒) ระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๒ (IAL2)

กำหนดให้มีการรวบรวมข้อมูลเพื่อระบุตัวตน พิจารณาหลักฐานแสดงตนโดยผู้พิสูจน์และยืนยันตัวตน และต้องตรวจสอบกับแหล่งให้ข้อมูลที่น่าเชื่อถือว่าไอเดนทิตีที่กล่าวอ้างมีอยู่ในโลกแห่งความจริง รวมถึงตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง การพิสูจน์ตัวตนที่ระดับ IAL2 สามารถทำได้ทั้งแบบพบเห็นต่อหน้า หรือแบบไม่พบเห็นต่อหน้า

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

๖.๒.๒ ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level: AAL)

ความปลอดภัยในการยืนยันตัวตนจะขึ้นอยู่กับจำนวนของปัจจัยของการยืนยันตัวตน โดยแบ่งสิ่งที่ใช้ยืนยันตัวตนได้เป็น ๒ แบบ ดังนี้

(๑) การยืนยันตัวตนแบบปัจจัยเดียว (single-factor authentication)

เป็นการยืนยันตัวตนที่ใช้สิ่งที่ใช้ยืนยันตัวตนเพียง ๑ ปัจจัย เช่น ผู้ใช้บริการแสดงรหัสผ่านในการเข้าระบบ ซึ่งรหัสผ่านเป็นสิ่งที่ผู้ใช้บริการรู้

(๒) การยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication)

เป็นการยืนยันตัวตนที่ใช้สิ่งที่ใช้ยืนยันตัวตนตั้งแต่ ๒ ปัจจัยขึ้นไปที่แตกต่างกันเพื่อเพิ่มความน่าเชื่อถือในการยืนยันตัวตนแต่ละครั้ง เช่น ผู้ใช้บริการแสดงรหัสผ่านเข้าระบบ ซึ่งรหัสผ่านเป็นสิ่งที่ผู้ใช้บริการรู้ และแสดงรหัสผ่านแบบใช้ครั้งเดียวที่ได้รับผ่านทางหมายเลขโทรศัพท์เคลื่อนที่ ซึ่งเป็นสิ่งที่ผู้ใช้บริการมี

จำนวนและประเภทของปัจจัยของการยืนยันตัวตนมีผลกับระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน โดยระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน คือ ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของผู้ใช้บริการ ซึ่งการกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนที่เหมาะสมจะช่วยลดโอกาสของการยืนยันตัวตนผิดพลาด แบ่งออกเป็น ๓ ระดับ ดังนี้

(๑) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ระดับที่ ๑ (AAL1)

กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบปัจจัยเดียวเป็นอย่างน้อย หรือหากต้องการความมั่นคงปลอดภัยที่สูงขึ้น สามารถยืนยันตัวตนแบบหลายปัจจัยได้ และต้องเป็นโพรโทคอลที่มีความปลอดภัย (secure authentication protocol) เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงต่ำ

(๒) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ระดับที่ ๒ (AAL2)

กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบ ๒ ปัจจัยที่แตกต่างกัน ซึ่งอาจเป็น (๑) สิ่งที่ใช้ยืนยันตัวตนหลายปัจจัย เช่น อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device) ซึ่งจะสร้างรหัสผ่านแบบใช้ครั้งเดียวหลังจากตรวจสอบลายนิ้วมือของผู้ใช้บริการ หรือ (๒) สิ่งที่ใช้ยืนยันตัวตนแบบปัจจัยเดียว อย่างน้อย ๒ สิ่งที่เป็นปัจจัยต่างกัน เช่น รหัสผ่าน (something you know) ควบคู่กับการใช้ OTP ผ่านหมายเลขโทรศัพท์เคลื่อนที่ (something you have) โดยโพรโทคอลที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตนต้องเป็นโพรโทคอลที่มีความปลอดภัย เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงปานกลางถึงความเสี่ยงสูง

(๓) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ระดับที่ ๓ (AAL3)

กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบ ๒ ปัจจัยขึ้นไปที่แตกต่างกัน โดยมีปัจจัยหนึ่งเป็นกุญแจที่ผ่านเกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol) ซึ่งผู้ใช้บริการต้องพิสูจน์ว่าตนครอบครองกุญแจนั้น และต้องพิสูจน์ว่าตนครอบครองปัจจัยของการยืนยันตัวตนดังกล่าว ผ่านโพรโทคอลที่มีความปลอดภัยในการใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน และต้องมีการเข้ารหัสข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหว (sensitive data) รวมถึงสิ่งที่ใช้ยืนยันตัวตนเพื่อป้องกันการปลอมแปลง เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงสูง

๖.๒.๓ ข้อกำหนดของการเลือกระดับความน่าเชื่อถือของไอเดนทิตีและระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

ในการเลือกระดับความน่าเชื่อถือสามารถทำแยกจากกันได้ เพื่อให้เกิดความยืดหยุ่นในการให้บริการของหน่วยงานของรัฐ อย่างไรก็ตาม มีข้อจำกัดเกี่ยวกับข้อมูลส่วนบุคคลของผู้ใช้บริการที่ใช้ลงทะเบียนกับผู้พิสูจน์และยืนยันตัวตน และสิ่งที่ใช้ยืนยันตัวตนที่จะป้องกันการเข้าถึงข้อมูลดังกล่าวจากบุคคลที่ไม่ได้รับอนุญาตต้องมีความสอดคล้องกัน ดังนั้น ต้องมีการจัดกลุ่มการใช้ระดับความน่าเชื่อถือของไอเดนทิตี และระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนบางระดับ เพื่อให้สามารถใช้งานร่วมกันได้ ดังตารางที่ ๑

ตารางที่ ๑ ระดับ IAL และ AAL ที่สามารถใช้งานร่วมกันได้

	AAL1	AAL2	AAL3
IAL1: ไม่มีข้อมูลส่วนบุคคล	สามารถใช้ได้	สามารถใช้ได้	สามารถใช้ได้
IAL1: มีข้อมูลส่วนบุคคล	ไม่สามารถใช้ได้	สามารถใช้ได้	สามารถใช้ได้
IAL2	ไม่สามารถใช้ได้	สามารถใช้ได้	สามารถใช้ได้
IAL3	ไม่สามารถใช้ได้	สามารถใช้ได้	สามารถใช้ได้

๖.๓ ความเสี่ยงและผลกระทบ (Risk and Impacts)

การประเมินความเสี่ยง (risk assessment) เป็นการวิเคราะห์และประเมินระดับความเสี่ยงที่ส่งผลกระทบเมื่อมีการพิสูจน์หรือยืนยันตัวตนผิดพลาด โดยพิจารณาจากระดับผลกระทบ (impact) และโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น (likelihood) [๑][๑๑] โดยผู้ให้บริการภาครัฐต้องพิจารณาถึงผลกระทบ ระดับความรุนแรง และโอกาสหรือความเป็นไปได้ที่อาจจะเกิดขึ้นได้หากการพิสูจน์หรือยืนยันตัวตนผิดพลาด ทั้งนี้ ผลลัพธ์ที่ได้จะนำใช้ในการกำหนดระดับความน่าเชื่อถือของไอเดนทิตีและระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน โดยดำเนินการ ดังนี้

๖.๓.๑ ระบุประเภทของผลกระทบ (categories of harm)

จากข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ [๔] แบ่งประเภทของผลกระทบเป็น ๖ ด้าน ดังนี้

(๑) ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง

(๒) ความเสียหายทางการเงิน

(๓) ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ

(๔) การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

(๕) ความปลอดภัยของบุคคล

(๖) การละเมิดทางแพ่งหรือทางอาญา

ทั้งนี้ อาจเพิ่มเติมประเภทของผลกระทบอื่น ๆ ให้สอดคล้องกับนโยบายด้านความเสี่ยงของหน่วยงานของตนได้

๖.๓.๒ วิเคราะห์ผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาดในแต่ละด้าน (impact levels)

การประเมินระดับผลกระทบที่เป็นไปได้ จะใช้วิธีการพิจารณาระดับผลกระทบที่สามารถเกิดขึ้นได้เมื่อเกิดข้อผิดพลาดในแต่ละด้าน ดังตารางที่ ๒

ตารางที่ ๒ เกณฑ์การพิจารณาระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด

ผลกระทบ	ระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด		
	ต่ำ	ปานกลาง	สูง
ความไม่สะดวกสบายและเสื่อมเสียชื่อเสียง	มีความไม่สะดวกสบายและเสื่อมเสียชื่อเสียงในระยะสั้น และจำกัด	มีความไม่สะดวกสบายและเสื่อมเสียชื่อเสียงที่รุนแรงในระยะสั้น หรือมีผลปานกลางในระยะยาว	มีความไม่สะดวกสบายและเสื่อมเสียชื่อเสียงในระยะยาว หรือมีผลกระทบหลายบุคคล
ความเสียหายทางการเงิน	มีความเสียหายทางการเงินที่ไม่มีนัยสำคัญ	มีความเสียหายทางการเงินรุนแรง	มีความเสียหายทางการเงินรุนแรงมาก
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบที่จำกัดต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงมากต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับถูกเปิดเผยและมีผลกระทบระดับต่ำ	มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับถูกเปิดเผยและมีผลกระทบระดับปานกลาง	มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับถูกเปิดเผยและมีผลกระทบระดับสูง
ความปลอดภัยของบุคคล	บาดเจ็บเล็กน้อยไม่ต้องรับการรักษาพยาบาล	มีความเสี่ยงพอสมควรที่จะบาดเจ็บเล็กน้อย หรือมีความเสี่ยงจำกัดที่จะบาดเจ็บซึ่งต้องการการรักษาพยาบาล	มีความเสี่ยงที่จะบาดเจ็บสาหัสหรือถึงแก่ชีวิต
การละเมิดทางแพ่งหรือทางอาญา	การฝ่าฝืนกฎหมายนั้นเป็นเรื่องเล็กน้อยซึ่งไม่จำเป็นต้องมีการบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงที่จะถูกบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงสูงเป็นพิเศษในการที่จะถูกบังคับใช้กฎหมาย

๖.๓.๓ กำหนดระดับโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น (likelihood levels)

ใช้วิธีการพิจารณาระดับโอกาสหรือความเป็นไปได้ที่จะเกิดผลกระทบที่สามารถเกิดขึ้นได้ในแต่ละด้าน ดังตารางที่ ๓

ตารางที่ ๓ เกณฑ์การพิจารณาโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น

โอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น	คะแนน	ความหมาย
สูง	๓	มีโอกาสเกิดขึ้นเป็นประจำ บ่อยครั้ง
ปานกลาง	๒	มีโอกาสเกิดบางครั้ง
ต่ำ	๑	มีโอกาสเกิด แต่นาน ๆ ครั้ง

๖.๓.๔ วัดผลความเสี่ยง (risk evaluation)

พิจารณาจากความสัมพันธ์ระหว่างผลกระทบและโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้นว่ามีความเสี่ยงระดับใด โดยมีสูตรการคำนวณดังนี้

ความเสี่ยง = โอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น x ผลกระทบ

โดยมีรายละเอียดเกณฑ์การวัดผลความเสี่ยง ดังตารางที่ ๔

ตารางที่ ๔ เกณฑ์การวัดผลความเสี่ยง

โอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น	ผลกระทบ		
	ต่ำ	ปานกลาง	สูง
สูง	๓	๖	๙
ปานกลาง	๒	๔	๖
ต่ำ	๑	๒	๓

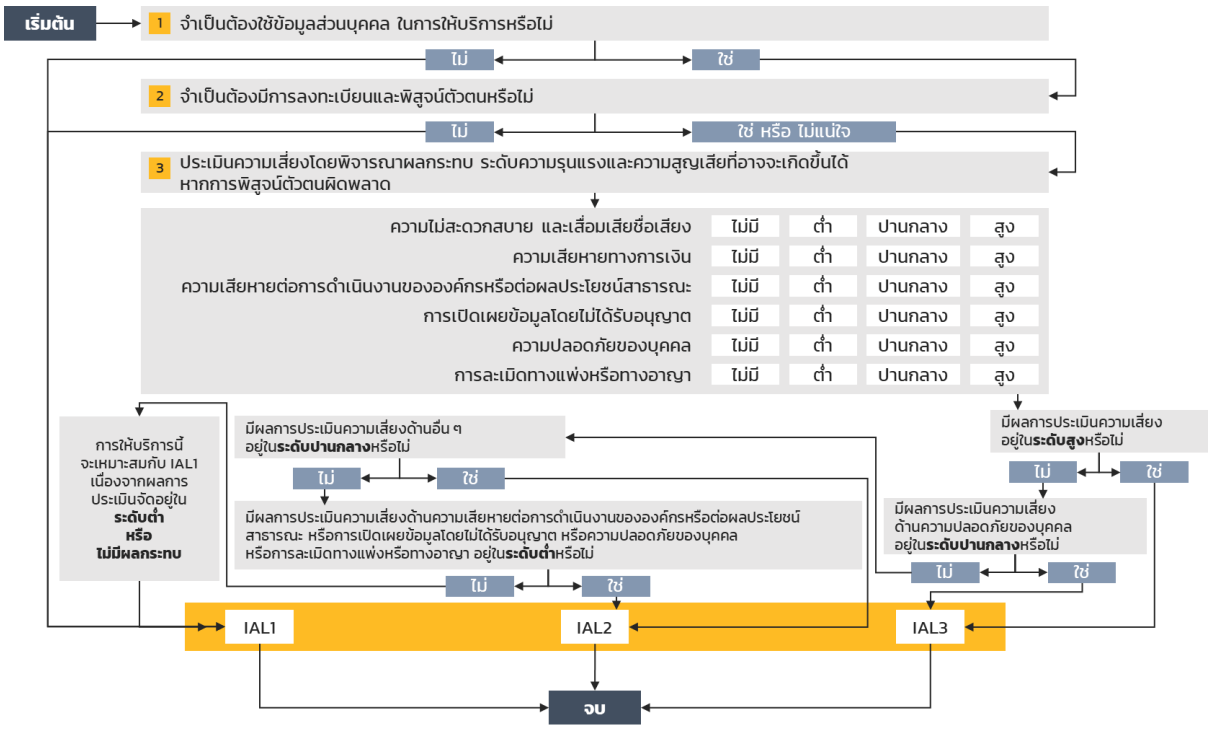
จากนั้น พิจารณาความหมายของแต่ละระดับความเสี่ยง ดังตารางที่ ๕

ตารางที่ ๕ ความหมายของแต่ละระดับความเสี่ยง

ระดับความเสี่ยง	ระดับคะแนน	แทนด้วย	ความหมาย
สูง	๖ - ๙		ระดับความเสี่ยงที่หน่วยงานของรัฐไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
ปานกลาง	๒ - ๔		ระดับความเสี่ยงที่หน่วยงานของรัฐสามารถยอมรับได้ โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยงเพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น
ต่ำ	๑		ระดับความเสี่ยงที่หน่วยงานของรัฐสามารถยอมรับได้ โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้

๗. การกำหนดระดับความน่าเชื่อถือของไอเดนทิตี (Selecting Identity Assurance Levels)

ผู้ให้บริการภาครัฐต้องกำหนดระดับความน่าเชื่อถือของไอเดนทิตี โดยนำผลของการประเมินความเสี่ยงมาประกอบการพิจารณาเพิ่มเติมที่เกี่ยวข้องกับการพิสูจน์ตัวตน เพื่อให้ผู้ให้บริการภาครัฐเลือกข้อกำหนดของการพิสูจน์ตัวตนที่เหมาะสมที่สุดสำหรับการให้บริการภาครัฐ



รูปที่ ๔ การกำหนดระดับความน่าเชื่อถือของไอเดนทิตี

ที่มา: ปรับปรุงจาก (NIST, NIST Special Publication 800-63-3 – Digital Identity Guidelines, 2017) [๑]

จากรูปที่ ๔ สามารถเชื่อมโยงผลการประเมินความเสี่ยง เพื่อนำมาพิจารณาระดับความน่าเชื่อถือของไอเดนทิตีที่เหมาะสม และสรุปได้ดังตารางที่ ๖ ดังนี้

(๑) กรณีที่ผลกระทบที่เป็นไปได้ด้านในด้านหนึ่งอยู่ในระดับสูง ให้กำหนดเป็น **ระดับ** IAL3

(๒) กรณีที่ผลกระทบด้านความปลอดภัยของบุคคลอยู่ในระดับปานกลาง ให้กำหนดเป็น **ระดับ** IAL3

(๓) กรณีที่ผลกระทบด้านอื่น ๆ อยู่ในระดับปานกลาง ให้กำหนดเป็น **ระดับ** IAL2

(๔) กรณีที่ผลกระทบด้านความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต หรือความปลอดภัยของบุคคล หรือการละเมิดทางแพ่งหรือทางอาญาอยู่ในระดับต่ำ ให้กำหนดเป็น **ระดับ** IAL2

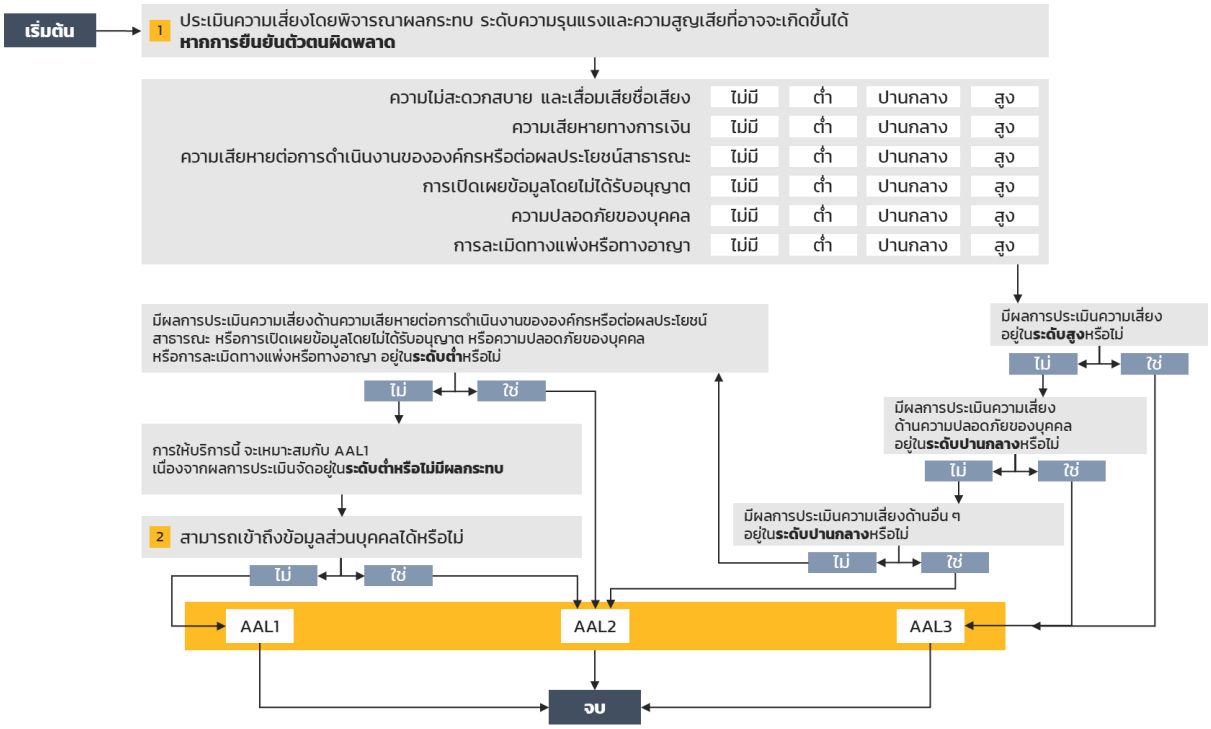
(๕) กรณีที่นอกเหนือจากนี้ ให้กำหนดเป็น **ระดับ** IAL1

ตารางที่ ๖ การจัดระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือของไอเดนทิตีของผลกระทบ

ผลกระทบ	ระดับความน่าเชื่อถือของไอเดนทิตี		
	๑	๒	๓
ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง	ต่ำ	ปานกลาง	สูง
ความเสียหายทางการเงิน	ต่ำ	ปานกลาง	สูง
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	ไม่มี	ต่ำ / ปานกลาง	สูง
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	ไม่มี	ต่ำ / ปานกลาง	สูง
ความปลอดภัยของบุคคล	ไม่มี	ต่ำ	ปานกลาง / สูง
การละเมิดทางแพ่งหรือทางอาญา	ไม่มี	ต่ำ / ปานกลาง	สูง

๘. การกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Selecting Authenticator Assurance Levels)

ผู้ให้บริการภาครัฐต้องกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน โดยนำผลของการประเมินความเสี่ยงมาประกอบกับการพิจารณาเพิ่มเติมที่เกี่ยวข้องกับการยืนยันตัวตน เพื่อให้ผู้ให้บริการภาครัฐเลือกข้อกำหนดของการยืนยันตัวตนที่เหมาะสมที่สุดสำหรับการให้บริการภาครัฐ



รูปที่ ๕ การกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

ที่มา: ปรับปรุงจาก (NIST, NIST Special Publication 800-63-3 – Digital Identity Guidelines, 2017) [๑]

จากรูปที่ ๕ สามารถเชื่อมโยงผลการประเมินความเสี่ยง เพื่อนำมาพิจารณาระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนที่เหมาะสม และสรุปได้ดังตารางที่ ๗ ดังนี้

(๑) กรณีที่ผลกระทบที่เป็นไปได้ด้านในด้านหนึ่งอยู่ในระดับสูง ให้กำหนดเป็น **ระดับ** AAL3

(๒) กรณีที่ผลกระทบด้านความปลอดภัยของบุคคลอยู่ในระดับปานกลาง ให้กำหนดเป็น **ระดับ** AAL3

(๓) กรณีที่ผลกระทบด้านอื่น ๆ อยู่ในระดับปานกลาง ให้กำหนดเป็น **ระดับ** AAL2

(๔) กรณีที่ผลกระทบด้านความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต หรือความปลอดภัยของบุคคล หรือการละเมิดทางแพ่งหรือทางอาญาอยู่ในระดับต่ำ ให้กำหนดเป็น **ระดับ** AAL2

(๕) กรณีที่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ ใช่หรือไม่ ถ้าใช่ ให้กำหนดเป็น **ระดับ** AAL2

(๖) กรณีที่นอกเหนือจากนี้ ให้กำหนดเป็น **ระดับ** AAL1

ตารางที่ ๗ การจัดระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนของผลกระทบ

ผลกระทบ	ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน		
	๑	๒	๓
ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง	ต่ำ	ปานกลาง	สูง
ความเสียหายทางการเงิน	ต่ำ	ปานกลาง	สูง
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	ไม่มี	ต่ำ / ปานกลาง	สูง
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	ไม่มี	ต่ำ / ปานกลาง	สูง
ความปลอดภัยของบุคคล	ไม่มี	ต่ำ	ปานกลาง / สูง
การละเมิดทางแพ่งหรือทางอาญา	ไม่มี	ต่ำ / ปานกลาง	สูง

ทั้งนี้ กรณีที่ผู้พิสูจน์และยืนยันตัวตนเป็นหน่วยงานของรัฐต้องดำเนินการให้เป็นไปตามแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย และต้องบริหารความเสี่ยงที่เหมาะสมและสอดคล้องกับความเสี่ยงของบริการภาครัฐ ซึ่งวิธีการพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้าและแบบเสมือนพบเห็นต่อหน้าอาจมีความเสี่ยงสูงกว่าแบบพบเห็นต่อหน้า ดังนั้นจึงต้องพิสูจน์ตัวตนในระดับที่เข้มข้นกว่า รวมถึงอาจมีวิธีการอื่น ๆ เพื่อช่วยบริหารความเสี่ยงที่อาจเกิดขึ้นได้

หากกรณีที่ผู้พิสูจน์และยืนยันตัวตนเป็นหน่วยงานของเอกชนต้องดำเนินการตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

อนึ่ง เมื่อผู้ให้บริการภาครัฐพิจารณากลุ่มการให้บริการภาครัฐ ระดับความน่าเชื่อถือของไอเดนทิตีและรูปแบบการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลสำหรับบริการภาครัฐแล้ว ให้ผู้ให้บริการภาครัฐและผู้พิสูจน์และยืนยันตัวตน จัดให้มีข้อตกลงในการดำเนินการและปฏิบัติตามข้อตกลงนั้น

บรรณานุกรม

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

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

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

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

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

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

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

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

[๙] ธนาคารแห่งประเทศไทย. (๒๕๖๒). *หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน*. ประกาศธนาคารแห่งประเทศไทย ที่ สนส. ๑๙/๒๕๖๒ ประกาศ ณ วันที่ ๒๓ สิงหาคม ๒๕๖๒ คัดจากราชกิจจานุเบกษา เล่มที่ ๑๓๖ ตอนพิเศษ ๒๑๙ ง วันที่ ๒ กันยายน ๒๕๖๒.

[๑๐] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (๒๕๖๑). *ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทำธุรกรรมแบบพบเห็นลูกค้าต่อหน้าสำหรับธนาคาร*. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

[๑๑] International Organization for Standardization. (2013). *Information technology - Security techniques - Information security management systems* (ISO/IEC27001). 2nd Edition.

มาตรฐานรัฐบาลดิจิทัล
DIGITAL GOVERNMENT STANDARD

มรด. ๑ - ๒ : ๒๕๖๔
DGS 1 - 2 : 2564

ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

DIGITALIZATION: DIGITAL ID - IDENTITY PROOFING AND AUTHENTICATION

เวอร์ชัน ๑.๐

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
สำนักนายกรัฐมนตรี

มาตรฐานรัฐบาลดิจิทัล
ว่าด้วยแนวทางการจัดทำกระบวนการ และการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

มรด. ๑ - ๒ : ๒๕๖๔

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
อาคารบางกอกไทยทาวเวอร์ ชั้น ๑๗
เลขที่ ๑๐๘ ถนนรางน้ำ แขวงถนนพญาไท เขตราชเทวี กรุงเทพมหานคร ๑๐๔๐๐
หมายเลขโทรศัพท์: ๐ ๒๖๑๒ ๖๐๐๐ โทรสาร: ๐ ๒๖๑๒ ๖๐๑๑, ๐ ๒๖๑๒ ๖๐๑๒

ประกาศโดย
คณะกรรมการพัฒนารัฐบาลดิจิทัล
วันที่ ๑๖ กันยายน ๒๕๖๔

คณะกรรมการพัฒนารัฐบาลดิจิทัล

ประธานกรรมการ

นายกรัฐมนตรี ประธานกรรมการ
มอบหมายและมอบอำนาจให้รองนายกรัฐมนตรี (นายดอน ปรมัตถ์วินัย)

กรรมการ

รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ปลัดสำนักนายกรัฐมนตรี
ปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ผู้อำนวยการสำนักงบประมาณ
เลขาธิการคณะกรรมการข้าราชการพลเรือน
เลขาธิการคณะกรรมการพัฒนาระบบราชการ
เลขาธิการสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ
กรรมการผู้ทรงคุณวุฒิในคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม
กรรมการผู้ทรงคุณวุฒิในคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
กรรมการผู้ทรงคุณวุฒิในคณะกรรมการข้อมูลข่าวสารของราชการ
กรรมการผู้ทรงคุณวุฒิในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
กรรมการผู้ทรงคุณวุฒิในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

กรรมการและเลขานุการ

ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ช่วยเลขานุการ

เจ้าหน้าที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะอนุกรรมการสถาปัตยกรรมและมาตรฐานการพัฒนารัฐบาลดิจิทัล

ประธานอนุกรรมการ

นายสมคิด จิรานันตรัตน์

อนุกรรมการ

ผู้แทนกระทรวงเกษตรและสหกรณ์
ผู้แทนกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ผู้แทนกระทรวงสาธารณสุข
ผู้แทนกรมการปกครอง
ผู้แทนกรมบัญชีกลาง
ผู้แทนกรมศุลกากร
ผู้แทนสำนักงานคณะกรรมการกฤษฎีกา
ผู้แทนสำนักงานคณะกรรมการข้าราชการพลเรือน
ผู้แทนสำนักงานคณะกรรมการพัฒนาระบบราชการ
ผู้แทนสำนักงบประมาณ
ผู้แทนสำนักงานการตรวจเงินแผ่นดิน
ผู้แทนธนาคารแห่งประเทศไทย
ผู้ทรงคุณวุฒิด้านสถาปัตยกรรมและมาตรฐานการพัฒนารัฐบาลดิจิทัล
- ผู้ช่วยศาสตราจารย์ภุชงค์ อุทโยภาศ
- นายพณชิต กิตติปัญญางาม
- นายศรัณย์ สัมฤทธิ์เดชขจร

อนุกรรมการและเลขานุการร่วม

ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

ผู้ช่วยเลขานุการ

เจ้าหน้าที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

ประธานกรรมการ

ผู้ช่วยศาสตราจารย์ภุชงค์ อุทโยภาศ	มหาวิทยาลัยเกษตรศาสตร์

รองประธานกรรมการ

นายวิบูลย์ ภัทรพิบูล	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

กรรมการ

ผู้ช่วยศาสตราจารย์โษฑศ์รัตต ธรรมบุษดี	มหาวิทยาลัยมหิดล
ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย
นายสุทธิศักดิ์ ตันตะโยธิน	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
นายพณชิต กิตติปัญญางาม	สมาคมการค้าเพื่อส่งเสริมผู้ประกอบการเทคโนโลยีรายใหม่
นายมารุต บูรณรัช	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
นางสาวปณิศา เหลืองวรเมท	สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ
นางสาวพลอย เจริญสม	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายศุภโชค จันทรประทิน	
นางบุญยิ่ง ชั่งสัจจา	สำนักบริหารการทะเบียน กรมการปกครอง
นายณัฏฐา พาชัยยุทธ	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นายพัชโรดม ลิมปิษเฐียร	สำนักงานคณะกรรมการกฤษฎีกา
นางสาวพัชรี ไชยเรืองกิตติ	
นางสาวสุภร สุขะตุงคะ	สำนักงานการตรวจเงินแผ่นดิน
นางสาวพลอยรวี เกริกพันธ์กุล	สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
นายทรงพล ใหม่สาลี	สำนักงานสถิติแห่งชาติ
นางกาญจนา ภู่มาลี	

กรรมการและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ

ที่ปรึกษา

นายสุพจน์ เธียรวุฒิ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ผู้ช่วยศาสตราจารย์ภุชงค์ อุทโยภาศ	มหาวิทยาลัยเกษตรศาสตร์

ประธานคณะทำงาน

ผู้ช่วยศาสตราจารย์ณัฐวุฒิ หนูไพโรจน์	จุฬาลงกรณ์มหาวิทยาลัย

คณะทำงาน

นายเนติพงษ์ ตลับนาค	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ
นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายชาลี วรกุลพิพัฒน์	ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
รองศาสตราจารย์เกริก ภิรมย์โสภา	จุฬาลงกรณ์มหาวิทยาลัย
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงานและเลขานุการ

นางสาวอุรัชฎา เกตุพรหม	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

วิเคราะห์และจัดทำมาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

นางสาวอัญชลี โพธิ์อ่อน	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นางสาวนงลักษณ์ พลอยสุภา	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายภัทร วานิชทวีวัฒน์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นางสาววีรวรรณ วระแสง	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย ฉบับนี้ จัดทำขึ้นเพื่อเป็นข้อกำหนดและแนวทางในการพิสูจน์และยืนยันตัวตนทางดิจิทัลของผู้ใช้บริการที่ต้องการใช้บริการภาครัฐด้วยดิจิทัลไอดี เพื่อให้หน่วยงานที่เกี่ยวข้องกับการใช้ดิจิทัลไอดีมีความเข้าใจตรงกัน โดยพัฒนาตามแนวมาตรฐานของ

- NIST Special Publication 800-63A – Digital Identity Guidelines – Enrollment and Identity Proofing, National Institute of Standards and Technology, US Department of Commerce [๒]
- NIST Special Publication 800-63B – Digital Identity Guidelines – Authentication and Lifecycle Management, National Institute of Standards and Technology, US Department of Commerce [๓]
- ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน [๕]
- ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน [๖]

อีกทั้งได้มีการรับฟังความคิดเห็นจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้มาตรฐานรัฐบาลดิจิทัล ฉบับนี้มีความครบถ้วนสมบูรณ์ สามารถนำไปปรับใช้ในทางปฏิบัติได้

มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย ฉบับนี้ จัดทำขึ้นโดยคณะกรรมการจัดทำร่างร่างมาตรฐาน ข้อกำหนด และหลักเกณฑ์ ภายใต้พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ คณะทำงานเทคนิคด้านมาตรฐานความมั่นคงปลอดภัยภาครัฐ ร่วมกับ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
อาคารบางกอกไทยทาวเวอร์ ๑๐๘ ถนนรางน้ำ
แขวงถนนพญาไท เขตราชเทวี กรุงเทพฯ ๑๐๔๐๐
โทรศัพท์: ๐ ๒๖๑๒ ๖๐๐๐
โทรสาร: ๐ ๒๖๑๒ ๖๐๑๑, ๐ ๒๖๑๒ ๖๐๑๒
E-mail: contact@dga.or.th
Website: www.dga.or.th

คำนำ

การจัดทำกระบวนการและการดำเนินงานทางดิจิทัลของภาครัฐ เป็นการวางรูปแบบร่วมกัน เพื่อสร้างขั้นตอนการทำงาน พัฒนาบริการให้เป็นรูปแบบดิจิทัลแบบครบวงจร สามารถเชื่อมโยงข้อมูลระหว่างหน่วยงานได้ โดยมีการนำระบบเทคโนโลยีดิจิทัลมาใช้ในการทำงาน เป็นกลไกในการเพิ่มประสิทธิภาพในการให้บริการภาครัฐแก่ประชาชน เป็นการเพิ่มทางเลือกให้แก่ประชาชนในการขอรับบริการจากภาครัฐ ช่วยลดความผิดพลาด ยกระดับการทำงานของภาครัฐผ่านระบบดิจิทัลตั้งแต่ต้นจนจบได้อย่างสมบูรณ์ นำไปสู่การเป็นรัฐบาลดิจิทัลที่ไร้กระดาษ (paperless) ซึ่งกระบวนการหลักของการดำเนินงานทางดิจิทัลของภาครัฐ เริ่มตั้งแต่การพิสูจน์และยืนยันตัวตนทางดิจิทัลไปจนถึงการจัดส่งใบอนุญาตหรือเอกสารต่าง ๆ ทางดิจิทัล

การพิสูจน์และยืนยันตัวตนทางดิจิทัล เป็นกระบวนการแรกที่สำคัญในการเข้าสู่บริการภาครัฐ ซึ่งหน่วยงานของรัฐต้องประเมินความต้องการของหน่วยงานเพื่อพิจารณาว่าบริการใดบ้างที่จำเป็นต้องใช้ดิจิทัลไอดีในการพิสูจน์และยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐ โดยมาตรฐานรัฐบาลดิจิทัลที่เกี่ยวข้องกับการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ ประกอบด้วย

(๖) แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม (Digitalization: Digital ID – Overview)

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

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

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

(๑๐) แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการออกดิจิทัลไอดีสำหรับบริการภาครัฐ (Digitalization: Digital ID – Government Issued ID)

สารบัญ

สารบัญตาราง

สารบัญภาพ

มาตรฐานรัฐบาลดิจิทัล

ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

๑. ขอบข่าย

มาตรฐานรัฐบาลดิจิทัลฯ ฉบับนี้ เป็นแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย เป็นข้อกำหนดและแนวทางในการพิสูจน์และยืนยันตัวตนทางดิจิทัลของผู้ใช้บริการที่ต้องการใช้บริการภาครัฐด้วยดิจิทัลไอดี เพื่อให้หน่วยงานที่เกี่ยวข้องกับการใช้ดิจิทัลไอดีมีความเข้าใจตรงกัน โดยอ้างอิงข้อกำหนด ดังนี้

(๗) มาตรฐาน NIST Special Publication 800-63-3 – Digital Identity Guidelines [๑]

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

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

(๑๐) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ [๔]

(๑๑) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน [๕]

(๑๒) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน [๖]

(๑๓) ประกาศธนาคารแห่งประเทศไทย ที่ สนส. ๑๙/๒๕๖๒ เรื่อง หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน [๙]

(๑๔) ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทำธุรกรรมแบบพบเห็นลูกค้าต่อหน้าสำหรับธนาคาร [๑๐]

ในมาตรฐานรัฐบาลดิจิทัลฯ ฉบับนี้ รูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) [๑] มีดังนี้

– “ต้อง” (shall) ใช้ระบุสิ่งที่เป็นข้อกำหนด (requirement) ที่ต้องปฏิบัติตาม

– “ควร” (should) ใช้ระบุสิ่งที่เป็นข้อแนะนำ (recommendation)

– “อาจ” (may) ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้ (permission)

การลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล (Enrolment and Identity Proofing)

๒. 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)

๒.๑ ระดับความน่าเชื่อถือของไอเดนทิตี (Identity Assurance Level: IAL)

ระดับความน่าเชื่อถือของไอเดนทิตี คือ ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของผู้สมัครใช้บริการ การกำหนดระดับความน่าเชื่อถือของไอเดนทิตีที่เหมาะสมจะช่วยลดโอกาสของการพิสูจน์ตัวตนผิดพลาด โดยระดับความน่าเชื่อถือของไอเดนทิตี แบ่งออกเป็น ๓ ระดับ ดังนี้

(๑) ระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๑ (IAL1)

มีการรวบรวมข้อมูลเพื่อระบุตัวตน พิจารณาและตรวจสอบหลักฐานแสดงตนหรือไม่ก็ได้ ทั้งนี้ไม่มีข้อกำหนดในการแสดงตนและตรวจสอบตัวบุคคลโดยผู้พิสูจน์และยืนยันตัวตน เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงต่ำ

(๒) ระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๒ (IAL2)

กำหนดให้มีการรวบรวมข้อมูลเพื่อระบุตัวตน พิจารณาหลักฐานแสดงตน โดยผู้พิสูจน์และยืนยันตัวตนต้องตรวจสอบกับแหล่งให้ข้อมูลที่น่าเชื่อถือว่าไอเดนทิตีที่กล่าวอ้างมีอยู่ในโลกแห่งความจริง รวมถึงตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง การพิสูจน์ตัวตนที่ระดับ IAL2 สามารถทำได้ทั้งแบบพบเห็นต่อหน้า หรือแบบไม่พบเห็นต่อหน้า

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

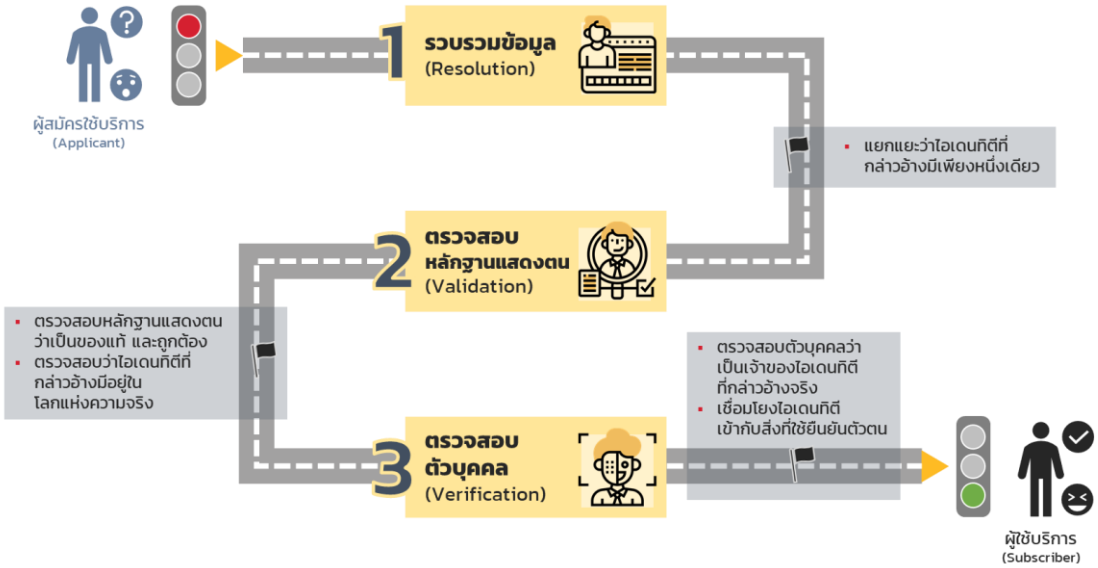
๒.๒ ขั้นตอนการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล (Process Flow)

เพื่อให้ขั้นตอนการรวบรวมและตรวจสอบข้อมูลหลักฐานแสดงตนของผู้สมัครใช้บริการมีคุณภาพเพียงพอที่จะมั่นใจว่า (๑) ผู้สมัครใช้บริการมีตัวตนจริงและมีเพียงหนึ่งเดียว (๒) หลักฐานเป็นของแท้ มีข้อมูลถูกต้อง และ (๓) ผู้สมัครใช้บริการเป็นเจ้าของหลักฐานที่นำมาแสดง มีกระบวนการดำเนินการ ดังนี้

(๑) การรวบรวมข้อมูลเพื่อระบุตัวตน เป็นกระบวนการที่ผู้พิสูจน์และยืนยันตัวตนรวบรวมคุณลักษณะและหลักฐานแสดงตนที่จำเป็นจากผู้สมัครใช้บริการ เพื่อแยกแยะว่าไอเดนทิตีของผู้สมัครใช้บริการมีเพียงหนึ่งเดียวและมีความเฉพาะเจาะจงภายในบริบทของผู้ใช้บริการทั้งหมดที่ผู้พิสูจน์และยืนยันตัวตนดูแล ทั้งนี้ การระบุตัวตนที่ดีควรใช้ชุดของคุณลักษณะเท่าที่จำเป็นในการแยกแยะไอเดนทิตีของผู้สมัครใช้บริการแต่ละราย

(๒) การตรวจสอบหลักฐานแสดงตน เป็นกระบวนการที่ผู้พิสูจน์และยืนยันตัวตนตรวจสอบความแท้จริง สถานะการใช้งาน และความถูกต้องของหลักฐานแสดงตน รวมถึงตรวจสอบข้อมูลที่อยู่ในหลักฐานแสดงตนว่าเป็นของบุคคลที่มีตัวตนอยู่จริง

(๓) การตรวจสอบตัวบุคคล เป็นกระบวนการที่ผู้พิสูจน์และยืนยันตัวตนตรวจสอบตัวบุคคลที่แสดงหลักฐานแสดงตน ว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างจริง โดยอาจมีการตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการที่ได้ให้ไว้ในขั้นตอนการลงทะเบียนว่าเป็นเจ้าของช่องทางที่ใช้ในการติดต่อจริง 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 โดยใช้ชุดของคุณลักษณะที่ใช้ระบุตัวตนให้น้อยที่สุดเท่าที่จำเป็นเพื่อแยกแยะไอเดนทิตีที่กล่าวอ้างออกจากไอเดนทิตีอื่น ซึ่งการรวบรวมข้อมูลเพื่อระบุตัวตนถือเป็นจุดเริ่มต้นของกระบวนการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล เช่น

(๑.๑) รวบรวมข้อมูลส่วนบุคคลจากผู้สมัครใช้บริการ เช่น เลขประจำตัวประชาชน ชื่อ ชื่อสกุล วันเดือนปีเกิด เลขหลังบัตรประจำตัวประชาชน อีเมล หมายเลขโทรศัพท์เคลื่อนที่

(๑.๒) รวบรวมหลักฐานแสดงตน เช่น บัตรประจำตัวประชาชนหรือหนังสือเดินทาง โดยอาจมีการทำสำเนาหรือถ่ายภาพไว้เป็นหลักฐาน

(๒) ตรวจสอบหลักฐานแสดงตน (validation)

การตรวจสอบหลักฐานแสดงตนมีจุดมุ่งหมายเพื่อรวบรวมหลักฐานการระบุตัวตนที่เหมาะสมที่สุดจากผู้สมัครใช้บริการเพื่อแสดงถึงความเป็นของแท้ สมบูรณ์ และถูกต้อง ซึ่งขั้นตอนของการตรวจสอบหลักฐานแสดงตน ประกอบด้วย การรวบรวมหลักฐานแสดงตนที่เหมาะสม การยืนยันหลักฐานแสดงตนว่าเป็นของแท้ และการยืนยันข้อมูลของหลักฐานแสดงตนว่าถูกต้อง เป็นปัจจุบัน และไอเดนทิตีที่กล่าวอ้างมีอยู่ในโลกแห่งความจริง เช่น

(๒.๑) ตรวจสอบข้อมูลที่ได้จากการรวบรวมข้อมูลตามข้อ (๑) กับแหล่งให้ข้อมูลที่น่าเชื่อถือโดยผู้พิสูจน์และยืนยันตัวตนต้องประเมินข้อมูลที่ได้รับจากผู้สมัครใช้บริการว่าตรงกัน

(๒.๒) ตรวจสอบสำเนาหรือภาพถ่ายของหลักฐานแสดงตนว่าไม่มีการปลอมแปลงแก้ไข เช่น เลขประจำตัวประชาชนที่อยู่ในสำเนาหรือภาพถ่ายต้องอยู่ในรูปแบบมาตรฐานที่กรมการปกครองกำหนด

(๒.๓) ตรวจสอบข้อมูลกับแหล่งออกหลักฐานแสดงตนว่าตรงกัน

(๓) ตรวจสอบตัวบุคคล (verification)

การตรวจสอบตัวบุคคลมีจุดมุ่งหมายเพื่อยืนยันและเชื่อมโยงระหว่างไอเดนทิตีที่กล่าวอ้างกับบุคคลที่ยื่นหลักฐานแสดงตนว่าตรงกันและมีตัวตนอยู่ในโลกแห่งความจริง เช่น

(๓.๑) ให้ผู้สมัครใช้บริการถ่ายภาพตนเอง เพื่อพิสูจน์ความเป็นบุคคลและสังเกตพฤติกรรม (liveness check) และตรวจสอบกับหลักฐานแสดงตนว่าตรงกัน

(๓.๒) นำภาพถ่ายจากหลักฐานแสดงตนเทียบกับภาพถ่ายของผู้สมัครใช้บริการว่าตรงกัน

(๓.๓) อาจมีการส่งรหัสการลงทะเบียนไปยังหมายเลขโทรศัพท์เคลื่อนที่ของผู้สมัครใช้บริการ โดยให้ผู้สมัครใช้บริการยืนยันรหัสการลงทะเบียนกลับมายังผู้พิสูจน์และยืนยันตัวตนโดยผู้พิสูจน์และยืนยันตัวตนเป็นผู้ยืนยันว่ารหัสดังกล่าวตรงกัน เพื่อเป็นการตรวจสอบว่าหมายเลขโทรศัพท์เคลื่อนที่นั้นเป็นของผู้สมัครใช้บริการจริง

๒.๓ ข้อกำหนดทั่วไป (General Requirements)

ข้อกำหนดทั่วไปสำหรับผู้พิสูจน์และยืนยันตัวตน ดำเนินการพิสูจน์ตัวตนของผู้สมัครใช้บริการที่มาขอใช้บริการว่าเป็นบุคคลรายนั้นจริง เพื่อป้องกันการทุจริตจากการปลอมแปลงหรือใช้ข้อมูลของบุคคลอื่นในการใช้บริการภาครัฐ ดังนี้

(๑) ต้องจัดให้ผู้สมัครใช้บริการแสดงตนและตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบันของข้อมูลและหลักฐานแสดงตนที่ได้รับจากผู้สมัครใช้บริการ รวมถึง ตรวจสอบว่าบุคคลที่มาสมัครใช้บริการภาครัฐเป็นบุคคลเดียวกันกับบุคคลในหลักฐานแสดงตน

(๒) ต้องบริหารความเสี่ยงให้เหมาะสมและสอดคล้องกับความเสี่ยงของบริการภาครัฐ โดยวิธีการพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้าและแบบเสมือนพบเห็นต่อหน้าอาจมีความเสี่ยงสูงกว่าแบบพบเห็นต่อหน้า จึงต้องพิสูจน์ตัวตนในระดับที่เข้มข้นกว่า รวมถึงจัดให้มีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อบริหารความเสี่ยงให้มีประสิทธิภาพมากขึ้น

(๓) ต้องกำหนดนโยบายและกระบวนการปฏิบัติงานภายในที่ชัดเจนเป็นลายลักษณ์อักษร โดยต้องทบทวน สื่อสาร ทำความเข้าใจ สร้างความตระหนักให้กับเจ้าหน้าที่หรือบุคลากรที่เกี่ยวข้องให้เห็นถึงความสำคัญ และปฏิบัติตามนโยบายและกระบวนการปฏิบัติงานภายในของผู้พิสูจน์และยืนยันตัวตนหรือหน่วยงานกำกับดูแลที่เกี่ยวข้อง นอกจากนี้ ต้องสื่อสารทำความเข้าใจและให้ความรู้กับผู้ใช้บริการด้วย

ทั้งนี้ ข้อกำหนดทั่วไปสำหรับผู้พิสูจน์และยืนยันตัวตนดำเนินการพิสูจน์ตัวตนที่ระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๒ หรือ ๓ ดังนี้

(๑) การพิสูจน์ตัวตนต้องไม่เป็นการประเมินถึงความเหมาะสม หรือการกำหนดสิทธิในการเข้าถึงบริการหรือสิทธิประโยชน์ต่าง ๆ

(๒) การรวบรวมข้อมูลส่วนบุคคลต้องรวบรวมให้น้อยที่สุดเท่าที่จำเป็น เพื่อตรวจสอบไอเดนทิตีที่กล่าวอ้างและเชื่อมโยงกับหลักฐานแสดงตนของผู้สมัครใช้บริการได้อย่างเหมาะสมสำหรับการรวบรวมข้อมูลเพื่อระบุตัวตน การตรวจสอบหลักฐานแสดงตน และการตรวจสอบตัวบุคคล ซึ่งอาจตรวจสอบหลักฐานแสดงตนกับแหล่งให้ข้อมูลที่น่าเชื่อถือและส่งให้ผู้ให้บริการภาครัฐใช้ในการตัดสินใจให้สิทธิเข้าใช้บริการ

(๓) ต้องแจ้งวัตถุประสงค์อย่างชัดเจนของการรวบรวมและจัดเก็บรักษาข้อมูลส่วนบุคคลที่ใช้สำหรับการพิสูจน์ตัวตนเท่าที่จำเป็น รวมถึงระบุคุณลักษณะที่ขึ้นอยู่กับความสมัครใจหรือคุณลักษณะที่จำเป็นต่อกระบวนการพิสูจน์ตัวตน และผลที่ตามมาหากผู้สมัครใช้บริการไม่แสดงคุณลักษณะดังกล่าว

(๔) ไม่นำคุณลักษณะที่รวบรวมและจัดเก็บในกระบวนการพิสูจน์ตัวตนไปใช้กับวัตถุประสงค์อื่นนอกเหนือจากการพิสูจน์ตัวตน การยืนยันตัวตน หรือปฏิบัติตามที่กฎหมายกำหนด โดยผู้พิสูจน์และยืนยันตัวตนต้องมีมาตรการในการรับมือกับความเสี่ยงที่อาจเกิดขึ้นกับความเป็นส่วนบุคคล เพื่อป้องกันไม่ให้เกิดการทำผิดกฎหมาย เว้นแต่ผู้พิสูจน์และยืนยันตัวตนได้แจ้งให้ผู้สมัครใช้บริการทราบอย่างชัดเจน และได้รับความยินยอมให้นำคุณลักษณะไปใช้กับ

วัตถุประสงค์อื่น 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 ต้องบันทึกประเภทหลักฐานแสดงตนที่นำมาแสดงตนในขั้นตอนของการพิสูจน์ตัวตน และต้องดำเนินการตามกระบวนการบริหารจัดการความเสี่ยง รวมถึงการประเมินความเสี่ยงด้านความเป็นส่วนบุคคลและความมั่นคงปลอดภัยเพื่อกำหนด ดังนี้

(๗.๑) ขั้นตอนเพิ่มเติมใด ๆ ที่ใช้ในการตรวจสอบไอเดนทิตีของผู้สมัครใช้บริการ นอกเหนือจากข้อกำหนดที่ต้องปฏิบัติตามซึ่งระบุไว้ในมาตรฐานรัฐบาลดิจิทัลฯ ฉบับนี้

(๗.๒) ข้อมูลส่วนบุคคล รวมถึงข้อมูลชีวมิติ รูปภาพ ภาพสแกน หรือสำเนาของหลักฐานแสดงตนอื่น ๆ ที่ผู้พิสูจน์และยืนยันตัวตนต้องจัดเก็บไว้เป็นบันทึกของการพิสูจน์ตัวตน

(๗.๓) 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 การจำกัดการใช้ข้อมูลและการแจ้งข้อมูลรวมถึงการใช้เทคโนโลยีเพื่อช่วยบรรเทาความเสี่ยง เช่น การเข้ารหัส (cryptography) และการจัดทำเอกสารตามข้อกำหนดที่ ๒.๓ (๗)

(๑๑)เมื่อกระบวนการลงทะเบียนและพิสูจน์ตัวตนสิ้นสุดลง ต้องกำจัดหรือทำลายข้อมูลอ่อนไหว (sensitive data) รวมถึงข้อมูลส่วนบุคคล หรือการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ตลอดช่วงระยะเวลาของเก็บรักษาข้อมูล

๒.๔ ข้อกำหนดวิธีการพิสูจน์ตัวตน (Identity Proofing Method Requirements)

ต้องนำข้อมูลและหลักฐานแสดงตนมาตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบัน รวมถึงตรวจสอบตัวบุคคลว่าเป็นผู้สมัครใช้บริการรายนั้นจริง โดยต้องดำเนินการดังนี้

๒.๔.๑ การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า

(๑) ต้องตรวจสอบหลักฐานแสดงตนว่ามีความถูกต้อง ความแท้จริง และยังมีสถานะใช้งานได้

(๒) กรณีผู้สมัครใช้บริการแสดงบัตรประจำตัวประชาชน ต้องตรวจสอบสถานะของข้อมูลและบัตรประจำตัวประชาชนของผู้สมัครใช้บริการที่เป็นปัจจุบันผ่านระบบให้บริการของแหล่งให้ข้อมูลที่น่าเชื่อถือ เพื่อทราบสถานะของข้อมูลและบัตรประจำตัวประชาชน

(๓) กรณีผู้สมัครใช้บริการแสดงหลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ต้องตรวจสอบความถูกต้อง ความแท้จริงของข้อมูลและหลักฐานแสดงตนด้วยเครื่องมืออิเล็กทรอนิกส์ เพื่อป้องกันการปลอมแปลงข้อมูลบนหน้าหลักฐานแสดงตน ทั้งนี้ หากผู้สมัครใช้บริการไม่มีหลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ หรือมีเหตุจำเป็นที่หลักฐานแสดงตนที่มีข้อมูลอิเล็กทรอนิกส์บกพร่อง ให้บริหารความเสี่ยงที่เกี่ยวข้องอย่างเหมาะสมและรัดกุม

(๔) กรณีผู้สมัครใช้บริการให้ช่องทางการติดต่อเป็นหมายเลขโทรศัพท์เคลื่อนที่ หรืออีเมล ต้องตรวจสอบหมายเลขโทรศัพท์เคลื่อนที่ หรืออีเมลดังกล่าวของผู้สมัครใช้บริการว่าสามารถติดต่อได้จริง

(๕) กรณีเลือกใช้วิธีการตรวจสอบลักษณะที่ปรากฏเทียบกับรูปถ่ายจากหลักฐานแสดงตน (physical comparison) ต้องตรวจสอบว่าตรงกับลักษณะที่ปรากฏของผู้สมัครใช้บริการเพื่อยืนยันว่าเป็นเจ้าของหลักฐานแสดงตนดังกล่าวจริง ทั้งนี้ กรณีผู้สมัครใช้บริการแสดงหลักฐานแสดงตนที่มีข้อมูลอิเล็กทรอนิกส์ ควรใช้รูปถ่ายที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์จากหลักฐานแสดงตนดังกล่าว เพื่อป้องกันการปลอมแปลงรูปถ่ายบนหน้าหลักฐานแสดงตน

(๖) กรณีเลือกใช้วิธีการตรวจสอบข้อมูลชีวมิติ (biometric comparison) เช่น ภาพใบหน้า หรือลายนิ้วมือ ต้องตรวจสอบเทียบกับข้อมูลชีวมิติจากหลักฐานแสดงตนว่าตรงกับผู้สมัครใช้บริการรายนั้นจริง

๒.๔.๒ การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า

(๑) ต้องตรวจสอบหลักฐานแสดงตนว่ามีความถูกต้อง ความแท้จริง และยังมีสถานะใช้งานได้

(๒) ต้องจัดให้มีกระบวนการลงทะเบียนและพิสูจน์ตัวตนผ่านระบบที่มีความน่าเชื่อถือ และมีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยในการตรวจสอบข้อมูลและหลักฐานแสดงตนของผู้สมัครใช้บริการเทียบเท่ากับการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า หรือเสมือนพบเห็นต่อหน้า

(๓) กรณีเลือกใช้วิธีการตรวจสอบลักษณะที่ปรากฏจากรูปถ่ายของผู้สมัครใช้บริการเทียบกับรูปถ่ายจากหลักฐานแสดงตน ต้องตรวจสอบว่าตรงกับลักษณะที่ปรากฏของผู้สมัครใช้บริการเพื่อยืนยันว่าเป็นเจ้าของหลักฐานแสดงตนดังกล่าวจริง

(๔) กรณีเลือกใช้วิธีการตรวจสอบข้อมูลชีวมิติ เช่น ภาพใบหน้า หรือลายนิ้วมือ อาจใช้เทคโนโลยีเพื่อพิสูจน์ความเป็นบุคคลและสังเกตพฤติกรรมผู้สมัครใช้บริการ (liveness detection) และเทคโนโลยีเปรียบเทียบข้อมูลชีวมิติของผู้สมัครใช้บริการ เพื่อพิสูจน์ว่าเป็นผู้สมัครใช้บริการรายนั้นจริงทดแทนการพบเห็นต่อหน้า ถ้าไม่สามารถสังเกตพฤติกรรมของผู้สมัครใช้บริการ ต้องกำหนดกระบวนการหรือแนวทางการบริหารความเสี่ยงเพิ่มเติมเพื่อลดความเสี่ยงจากกรณีทุจริตต่าง ๆ ได้

๒.๔.๓ การพิสูจน์ตัวตนแบบเสมือนพบเห็นต่อหน้า

(๑) ต้องตรวจสอบหลักฐานแสดงตนว่ามีความถูกต้อง ความแท้จริง และยังมีสถานะใช้งานได้

(๒) ต้องจัดให้มีกระบวนการลงทะเบียนและพิสูจน์ตัวตนผ่านระบบที่มีความน่าเชื่อถือและมีมาตรการหรือระบบรักษาความมั่นคงปลอดภัยในการตรวจสอบข้อมูลและหลักฐานแสดงตนของผู้สมัครใช้บริการเทียบเท่ากับการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า

(๓) ต้องจัดให้มีเจ้าหน้าที่ที่มีหน้าที่รับผิดชอบและผ่านการฝึกอบรม ทำหน้าที่เฝ้าสังเกตและเข้าร่วมสนทนาออนไลน์กับผู้สมัครใช้บริการแบบถ่ายทอดสดตลอดเวลาของการลงทะเบียนและพิสูจน์ตัวตน

๒.๕ ข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๑ (IAL1)

ผู้พิสูจน์และยืนยันตัวตนต้องดำเนินการตามข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๑ ดังนี้

(๑) รวบรวมข้อมูลส่วนบุคคลเพื่อระบุตัวตนของผู้สมัครใช้บริการหรือไม่ก็ได้

(๒) กรณีขอหลักฐานแสดงตนที่ยังไม่หมดอายุจากผู้สมัครใช้บริการ มีดังนี้

(๒.๑) บัตรประจำตัวประชาชน **หรือ**

(๒.๒) หนังสือเดินทาง **หรือ**

(๒.๓) หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ

(๓) ตรวจสอบข้อมูลหรือหลักฐานแสดงตนตามข้อ ๒.๕ (๒) ว่าเป็นของแท้ และถูกต้อง

(๔) ตรวจสอบช่องทางการติดต่อว่าสามารถติดต่อผู้สมัครใช้บริการได้

๒.๖ ข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๒ (IAL2)

ผู้พิสูจน์และยืนยันตัวตนต้องดำเนินการตามข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๒ ดังนี้

(๑) ต้องรองรับวิธีการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า **หรือ** ไม่พบเห็นต่อหน้า ทั้งนี้ควรจัดให้มีการพิสูจน์ตัวตนทั้งสองรูปแบบสำหรับการแสดงตนของผู้สมัครใช้บริการ

(๒) การรวบรวมข้อมูลเพื่อระบุตัวตน

(๒.๑) ต้องรวบรวมข้อมูลส่วนบุคคลของผู้สมัครใช้บริการเท่าที่จำเป็น เพื่อแยกแยะว่าไอเดนทิตีของผู้สมัครใช้บริการมีเพียงหนึ่งเดียวและมีความเฉพาะเจาะจงภายในบริบทของผู้ใช้บริการทั้งหมดที่ผู้พิสูจน์และยืนยันตัวตนดูแล ซึ่งอาจรวมถึงการรวบรวมคุณลักษณะ เพื่อช่วยในการค้นหาข้อมูล

(๒.๒) อาจใช้การยืนยันด้วยชุดข้อมูลที่รู้เฉพาะผู้สมัครใช้บริการ (knowledge-based verification: KBV)

(๓) ต้องขอหลักฐานแสดงตนที่ยังไม่หมดอายุจากผู้สมัครใช้บริการ ดังนี้

(๓.๑) บัตรประจำตัวประชาชน **หรือ**

(๓.๑) หนังสือเดินทาง **หรือ**

(๓.๑) หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ

(๔) การตรวจสอบหลักฐานแสดงตน

(๔.๑) ต้องตรวจสอบหลักฐานแสดงตนตาม ๒.๖ (๓) โดยใช้เจ้าหน้าที่หรือเทคโนโลยีที่เหมาะสมว่าเป็นของแท้

(๔.๑) ต้องตรวจสอบข้อมูลของหลักฐานแสดงตนตาม ๒.๖ (๓) โดยเปรียบเทียบกับข้อมูลจากแหล่งให้ข้อมูลที่น่าเชื่อถือว่ามีความถูกต้อง

(๕) การตรวจสอบตัวบุคคล

(๕.๑) ต้องตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง โดยเปรียบเทียบลักษณะที่ปรากฏของผู้สมัครใช้บริการกับรูปถ่ายจากหลักฐานแสดงตน **หรือ** เปรียบเทียบข้อมูลชีวมิติของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน

(๕.๑) อาจบันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (biometric sample) (เช่น ภาพใบหน้า ลายนิ้วมือ) เพื่อวัตถุประสงค์ในการห้ามปฏิเสธความรับผิด (non-repudiation) และการตรวจสอบอีกครั้งในกรณีจำเป็น (re-proofing)

(๖) การตรวจสอบช่องทางการติดต่อ

(๖.๑) ต้องตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถติดต่อได้จริง เช่น การตรวจสอบอีเมลด้วยวิธีการยืนยันทางอีเมล การตรวจสอบหมายเลขโทรศัพท์เคลื่อนที่ด้วยรหัสผ่านแบบใช้ครั้งเดียว (OTP) หรือวิธีการยืนยันทาง SMS

๒.๗ ข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๓ (IAL3)

ผู้พิสูจน์และยืนยันตัวตนต้องดำเนินการตามข้อกำหนดของระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๓ ดังนี้

(๑) ต้องพิสูจน์ตัวตนแบบพบเห็นต่อหน้า **หรือ** เสมือนพบเห็นต่อหน้า ทั้งนี้ควรจัดให้มีการพิสูจน์ตัวตนทั้งสองรูปแบบสำหรับการแสดงตนเพื่อระบุตัวตนของผู้สมัครใช้บริการ โดยมีข้อกำหนด ดังนี้

(๑.๑) ข้อกำหนดของการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า

(๑.๑.๑) ต้องมีเจ้าหน้าที่ที่มีหน้าที่รับผิดชอบและผ่านการฝึกอบรมทำหน้าที่สังเกตสิ่งผิดปกติบนร่างกายของผู้สมัครใช้บริการ (เช่น ใบหน้า นิ้วมือ) และดำเนินการตรวจสอบตามกระบวนการพิสูจน์ตัวตน

(๑.๑.๒) ต้องรวบรวมข้อมูลชีวมิติในลักษณะที่มั่นใจว่าข้อมูลชีวมิติดังกล่าวถูกรวบรวมจากผู้สมัครใช้บริการ และไม่ใช่จากบุคคลอื่น

(๑.๒) ข้อกำหนดของการพิสูจน์ตัวตนแบบเสมือนพบเห็นต่อหน้า

(๑.๒.๑) ต้องเฝ้าสังเกตผู้สมัครใช้บริการตลอดเวลาของการพิสูจน์ตัวตน โดยที่ผู้สมัครใช้บริการต้องไม่ออกไปจากการสื่อสาร เช่น การเฝ้าสังเกตผู้สมัครใช้บริการด้วยการส่งผ่านวิดีโอที่มีความละเอียดสูงอย่างต่อเนื่อง (high resolution video transmission)

(๑.๒.๒) ต้องมีเจ้าหน้าที่ที่มีหน้าที่รับผิดชอบและผ่านการฝึกอบรม ทำหน้าที่เฝ้าสังเกตและเข้าร่วมสนทนาออนไลน์กับผู้สมัครใช้บริการแบบถ่ายทอดสดตลอดเวลาของการพิสูจน์ตัวตน เช่น การส่งผ่านวิดีโอที่มีความละเอียดสูงอย่างต่อเนื่อง

(๑.๒.๓) เจ้าหน้าที่ต้องสามารถมองเห็นพฤติกรรมทั้งหมดของผู้สมัครใช้บริการระหว่างช่วงเวลาของการพิสูจน์ตัวตนได้อย่างชัดเจน

(๑.๒.๔) ต้องตรวจสอบหลักฐานแสดงตนด้วยวิธีการทางอิเล็กทรอนิกส์ โดยใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์หรือวิธีการที่เทียบเท่า เช่น การตรวจสอบลายมือชื่อที่ออกหลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ และใช้เครื่องมืออุปกรณ์ของผู้พิสูจน์และยืนยันตัวตนทั้งหมด

(๑.๒.๕) ต้องฝึกอบรมเจ้าหน้าที่เพื่อให้สามารถตรวจหาความผิดปกติที่อาจเกิดขึ้นในการพิสูจน์ตัวตน และดำเนินการได้อย่างเหมาะสม

(๑.๒.๖) ต้องติดตั้งระบบตรวจจับการบุกรุกทางกายภาพที่เหมาะสมกับสภาพแวดล้อมของสถานที่ตั้ง เช่น เครื่องให้บริการอัตโนมัติ (kiosk) ต้องตั้งอยู่ในพื้นที่ที่จำกัดหรือพื้นที่ที่มีการรักษาความมั่นคงปลอดภัย

(๑.๒.๗) ต้องตรวจสอบให้มั่นใจว่าการติดต่อสื่อสารทั้งหมดเกิดขึ้นผ่านช่องทางการสื่อสารเฉพาะที่มีการป้องกัน

(๒) การรวบรวมข้อมูลเพื่อระบุตัวตน

(๒.๑) ข้อกำหนดเช่นเดียวกับ IAL2

(๓) ต้องขอหลักฐานแสดงตนที่ยังไม่หมดอายุจากผู้สมัครใช้บริการ โดยมีทางเลือก ดังนี้

(๓.๑) บัตรประจำตัวประชาชนและหนังสือเดินทาง **หรือ**

(๓.๒) ใช้การตรวจสอบหลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ๒ ชิ้นขึ้นไป **หรือ**

(๓.๓) บัตรประจำตัวประชาชนและแหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่น ๒ แหล่งขึ้นไป

(๔) การตรวจสอบหลักฐานแสดงตน

(๔.๑) ข้อกำหนดเช่นเดียวกับ IAL2

(๕) การตรวจสอบตัวบุคคล

(๕.๑) ต้องตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง โดยเปรียบเทียบข้อมูลชีวมิติของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน

(๕.๒) ต้องบันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (เช่น ภาพใบหน้า ลายนิ้วมือ) เพื่อวัตถุประสงค์ในการห้ามปฏิเสธความรับผิด และการตรวจสอบอีกครั้งในกรณีจำเป็น

(๖) การตรวจสอบช่องทางการติดต่อ

(๖.๑) ข้อกำหนดเช่นเดียวกับ IAL2

๒.๘ สรุปข้อกำหนดระดับความน่าเชื่อถือของไอเดนทิตี (Summary of Requirements)

ข้อกำหนดระดับความน่าเชื่อถือของไอเดนทิตี สรุปได้ดังตารางที่ ๑

ตารางที่ ๑ สรุปข้อกำหนดระดับความน่าเชื่อถือของไอเดนทิตี

ข้อกำหนด	IAL1	IAL2	IAL3
การแสดงตน	ไม่มีข้อกำหนด	ต้องรองรับวิธีการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า **หรือ** ไม่พบเห็นต่อหน้า	ต้องพิสูจน์ตัวตนแบบพบเห็นต่อหน้า **หรือ** เสมือนพบเห็นต่อหน้า
การรวบรวมข้อมูลเพื่อระบุตัวตน	รวบรวมข้อมูลเพื่อระบุตัวตนหรือไม่ก็ได้	- ต้องรวบรวมข้อมูลเพื่อระบุตัวตน - อาจใช้ชุดข้อมูลที่รู้เฉพาะผู้สมัครใช้บริการ (knowledge-based verification : KBV)	เช่นเดียวกับ IAL2
การขอหลักฐานแสดงตน	ขอหลักฐานแสดงตนที่ยังไม่หมดอายุหรือไม่ก็ได้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ	ต้องขอหลักฐานแสดงตนที่ยังไม่หมดอายุ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ	ต้องขอหลักฐานแสดงตนที่ยังไม่หมดอายุ - ทางเลือกที่ ๑ บัตรประจำตัวประชาชน และ หนังสือเดินทาง **หรือ** - ทางเลือกที่ ๒ หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ๒ ชิ้นขึ้นไป **หรือ** - ทางเลือกที่ ๓ บัตรประจำตัวประชาชน และ แหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่น ๒ แหล่งขึ้นไป

ตารางที่ ๑ สรุปข้อกำหนดระดับความน่าเชื่อถือของไอเดนทิตี

(ต่อ)

ข้อกำหนด	IAL1	IAL2	IAL3
การตรวจสอบหลักฐานแสดงตน	ตรวจสอบและเปรียบเทียบหลักฐานแสดงตนที่ยังไม่หมดอายุว่าเป็นของแท้และถูกต้องหรือไม่ก็ได้	- ต้องตรวจสอบหลักฐานแสดงตนโดยใช้เจ้าหน้าที่หรือเทคโนโลยีที่เหมาะสมว่าเป็นของแท้ - ต้องตรวจสอบข้อมูลของหลักฐานแสดงตนโดยเปรียบเทียบกับข้อมูลจากแหล่งให้ข้อมูลที่น่าเชื่อถือว่ามีความถูกต้อง	เช่นเดียวกับ IAL2
การตรวจสอบตัวบุคคล	ไม่ตรวจสอบตัวบุคคล	ต้องตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง โดย - เปรียบเทียบลักษณะที่ปรากฏเทียบกับรูปถ่ายจากหลักฐานแสดงตน (physical comparison) **หรือ** - เปรียบเทียบภาพใบหน้าหรือลายนิ้วมือเทียบกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)	ต้องตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง โดย - เปรียบเทียบภาพใบหน้าหรือลายนิ้วมือเทียบกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)
การรวบรวมข้อมูลชีวมิติ	ไม่มีข้อกำหนด	บันทึกตัวอย่างข้อมูลชีวมิติ (biometric sample) หรือไม่ก็ได้	ต้องบันทึกตัวอย่างข้อมูลชีวมิติ (biometric sample)
การตรวจสอบช่องทางการติดต่อ	ตรวจสอบช่องทางการติดต่อว่าสามารถติดต่อได้ - หมายเลขโทรศัพท์เคลื่อนที่ **หรือ** - อีเมล	ต้องตรวจสอบช่องทางการติดต่อ - หมายเลขโทรศัพท์เคลื่อนที่ **หรือ** - อีเมล	เช่นเดียวกับ IAL2

๒.๙ ข้อกำหนดขั้นต่ำในการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล (Minimum Requirements for Enrolment and Identity Proofing)

ผู้พิสูจน์และยืนยันตัวตนระบุข้อกำหนดในการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลให้เป็นไปตามกลุ่มการให้บริการภาครัฐ ทั้ง ๔ กลุ่ม [๘] โดยต้องประเมินความต้องการของหน่วยงาน ความเสี่ยง และระดับความน่าเชื่อถือ โดยเลือกวิธีการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลที่เหมาะสม เพื่อให้ขั้นตอนการรวบรวม และตรวจสอบข้อมูลหลักฐานแสดงตนของผู้สมัครใช้บริการ มีคุณภาพเพียงพอที่จะให้มั่นใจว่า (๑) ผู้สมัครใช้บริการมีตัวตนจริงและมีเพียงหนึ่งเดียว (๒) หลักฐานเป็นของแท้ มีข้อมูลถูกต้อง และ (๓) ผู้สมัครใช้บริการเป็นเจ้าของหลักฐานที่นำมาแสดง

ข้อกำหนดขั้นต่ำในการกำหนดระดับความน่าเชื่อถือของไอเดนทิตีสำหรับการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล จำแนกตามกลุ่มการให้บริการภาครัฐ ดังนี้

(๑) กลุ่มการให้บริการข้อมูลพื้นฐาน จัดเป็นบริการที่ไม่มีความเสี่ยงหรือมีความเสี่ยงต่ำ จึง**ไม่จำเป็นต้องใช้ดิจิทัลไอดี**

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

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

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

หมายเหตุ *กรณีที่ต้องมีการตรวจสอบหลักฐานแสดงตนกับแหล่งให้ข้อมูลที่น่าเชื่อถือมากกว่า ๑ แหล่งขึ้นไป ให้มีการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เช่น ศูนย์แลกเปลี่ยนข้อมูลกลาง โดยไม่ต้องร้องขอข้อมูลจากผู้สมัครใช้บริการเพิ่มเติม*

อนึ่ง หากบริการภาครัฐใดที่ต้องใช้ข้อมูลส่วนบุคคลในการพิสูจน์และยืนยันตัวตน ให้กำหนดระดับความน่าเชื่อถือของไอเดนทิตีขั้นต่ำที่ระดับ ๒ ซึ่งเทียบเท่ากับระดับความน่าเชื่อถือของไอเดนทิตีที่ระดับ ๒.๑ ของประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย - การลงทะเบียนและพิสูจน์ตัวตน

รายละเอียดแนวทางการกำหนดระดับความน่าเชื่อถือของไอเดนทิตีของกลุ่มการให้บริการภาครัฐ ดังตารางที่ ๒

ตารางที่ ๒ แนวทางการกำหนดระดับความน่าเชื่อถือของไอเดนทิตีของกลุ่มการให้บริการภาครัฐ

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ	IAL1	การรวบรวมข้อมูลเพื่อระบุตัวตน	เจ้าหน้าที่รวบรวมข้อมูลเพื่อระบุตัวตนของผู้สมัครใช้บริการหรือไม่ก็ได้	เจ้าหน้าที่รวบรวมข้อมูลเพื่อระบุตัวตนของผู้สมัครใช้บริการผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดเพื่อแสดงตนหรือไม่ก็ได้	เจ้าหน้าที่รวบรวมข้อมูลเพื่อระบุตัวตนของผู้สมัครใช้บริการผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดเพื่อแสดงตนหรือไม่ก็ได้
		การตรวจสอบหลักฐานแสดงตน	IdP ตรวจสอบข้อมูลหลักฐานแสดงตนยังไม่หมดอายุหรือไม่ก็ได้ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ	IdP ตรวจสอบข้อมูลหลักฐานแสดงตนยังไม่หมดอายุหรือไม่ก็ได้ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ผู้สมัครใช้บริการถ่ายรูปหลักฐานแสดงตนผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดของ IdP และเจ้าหน้าที่ดูรูปหลักฐานแสดงตนเพื่อตรวจสอบว่าเป็นของแท้	IdP ตรวจสอบข้อมูลหลักฐานแสดงตนยังไม่หมดอายุหรือไม่ก็ได้ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ผู้สมัครใช้บริการถ่ายรูปหลักฐานแสดงตนผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดของ IdP และเจ้าหน้าที่ดูรูปหลักฐานแสดงตน เพื่อตรวจสอบว่าเป็นของแท้

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
				- เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลบนหลักฐานแสดงตนเพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง	- เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลบนหลักฐานแสดงตนเพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง
		การตรวจสอบตัวบุคคล	ไม่มีข้อกำหนด	ไม่มีข้อกำหนด	ไม่มีข้อกำหนด
		การตรวจสอบช่องทางการติดต่อ	IdP ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถติดต่อได้ เช่น อีเมล หมายเลขโทรศัพท์เคลื่อนที่	IdP ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถติดต่อได้ เช่น อีเมล หมายเลขโทรศัพท์เคลื่อนที่	IdP ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถติดต่อได้ เช่น อีเมล หมายเลขโทรศัพท์เคลื่อนที่
กลุ่มการให้บริการธุรกรรม	IAL2	การรวบรวมข้อมูลเพื่อระบุตัวตน	ผู้สมัครใช้บริการ <u>ต้อง</u>ให้ข้อมูลเพื่อแสดงตน โดยเจ้าหน้าที่รวบรวมข้อมูลเพื่อระบุตัวตน เช่น ชื่อ ชื่อสกุล ที่อยู่ อีเมล หมายเลขโทรศัพท์เคลื่อนที่	ผู้สมัครใช้บริการ <u>ต้อง</u>ให้ข้อมูลผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดของ IdP โดยเจ้าหน้าที่รวบรวมข้อมูลเพื่อระบุตัวตน	ผู้สมัครใช้บริการ <u>ต้อง</u>ให้ข้อมูลผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดของ IdP โดยเจ้าหน้าที่รวบรวมข้อมูลเพื่อระบุตัวตน
		การตรวจสอบหลักฐานแสดงตน	IdP <u>ต้อง</u>ตรวจสอบข้อมูลหลักฐานแสดงตนที่ยังไม่หมดอายุ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ	IdP <u>ต้อง</u>ตรวจสอบข้อมูลหลักฐานแสดงตนที่ยังไม่หมดอายุ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ	IdP <u>ต้อง</u>ตรวจสอบข้อมูลหลักฐานแสดงตนที่ยังไม่หมดอายุ ดังนี้ - บัตรประจำตัวประชาชน **หรือ** - หนังสือเดินทาง **หรือ** - หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
			- เจ้าหน้าที่ใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์เพื่อตรวจสอบหลักฐานแสดงตนว่าเป็นของแท้ - เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง	- ผู้สมัครใช้บริการใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์หรือเทคโนโลยีที่กำหนดของ IdP เพื่อตรวจสอบหลักฐานแสดงตนว่าเป็นของแท้ - IdP เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง	- ผู้สมัครใช้บริการใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์หรือเทคโนโลยีที่กำหนดของ IdP เพื่อตรวจสอบหลักฐานแสดงตนว่าเป็นของแท้ - เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง
		การตรวจสอบตัวบุคคล	- เจ้าหน้าที่อาจถ่ายรูปและบันทึกภาพใบหน้าของผู้สมัครใช้บริการเพื่อใช้เป็นหลักฐาน - เจ้าหน้าที่เปรียบเทียบลักษณะที่ปรากฏของผู้สมัครใช้บริการกับรูปถ่ายจากหลักฐานแสดงตน (physical comparison) - กรณีใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้า	- ผู้สมัครใช้บริการถ่ายรูปตัวเองพร้อมหลักฐานแสดงตนผ่านแอปพลิเคชันของ IdP และ IdP บันทึกภาพใบหน้าของผู้สมัครใช้บริการเพื่อใช้เป็นหลักฐาน - เจ้าหน้าที่เปรียบเทียบรูปถ่ายของผู้สมัครใช้บริการกับรูปถ่ายจากหลักฐานแสดงตน (physical comparison)	- ผู้สมัครใช้บริการถ่ายรูปตัวเองผ่านแอปพลิเคชัน เว็บไซต์หรือเทคโนโลยีที่กำหนดของ IdP และ IdP บันทึกภาพใบหน้าของผู้สมัครใช้บริการเพื่อใช้เป็นหลักฐาน - เจ้าหน้าที่เปรียบเทียบรูปถ่ายของผู้สมัครใช้บริการกับรูปถ่ายจาก

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
			หรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)	- กรณีใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)	หลักฐานแสดงตน (physical comparison) - กรณีใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)
		การตรวจสอบช่องทางการติดต่อ	IdP <u>ต้อง</u>ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง เช่น หมายเลขโทรศัพท์เคลื่อนที่ อีเมล	IdP <u>ต้อง</u>ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง เช่น หมายเลขโทรศัพท์เคลื่อนที่ อีเมล	IdP <u>ต้อง</u>ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง เช่น หมายเลขโทรศัพท์เคลื่อนที่ อีเมล
กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงานที่มีความเสี่ยงสูง	IAL3	การรวบรวมข้อมูลเพื่อระบุตัวตน	ผู้สมัครใช้บริการ<u>ต้อง</u>ให้ข้อมูลเพื่อแสดงตน โดยเจ้าหน้าที่รวบรวมข้อมูลเพื่อระบุตัวตน		ผู้สมัครใช้บริการ<u>ต้อง</u>ให้ข้อมูลผ่านแอปพลิเคชัน เว็บไซต์ หรือเทคโนโลยีที่กำหนดของ IdP โดยเจ้าหน้าที่รวบรวมข้อมูลเพื่อระบุตัวตน
		การตรวจสอบหลักฐานแสดงตน	IdP <u>ต้อง</u>ขอหลักฐานแสดงตนที่ยังไม่หมดอายุ ดังนี้		IdP <u>ต้อง</u>ขอหลักฐานแสดงตนที่ยังไม่หมดอายุ ดังนี้

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
			- ทางเลือกที่ ๑ บัตรประจำตัวประชาชน และ หนังสือเดินทาง **หรือ** - ทางเลือกที่ ๒ หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ๒ ชิ้นขึ้นไป **หรือ** - ทางเลือกที่ ๓ บัตรประจำตัวประชาชน และ แหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่น ๒ แหล่งขึ้นไป - เจ้าหน้าที่ดูหลักฐานแสดงตนและใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์ หรือตรวจสอบแหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่นเพื่อตรวจสอบว่าเป็นของแท้ - เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับ		- ทางเลือกที่ ๑ บัตรประจำตัวประชาชน และ หนังสือเดินทาง **หรือ** - ทางเลือกที่ ๒ หลักฐานแสดงตนในรูปแบบอิเล็กทรอนิกส์ที่น่าเชื่อถือ ๒ ชิ้นขึ้นไป **หรือ** - ทางเลือกที่ ๓ บัตรประจำตัวประชาชน และ แหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่น ๒ แหล่งขึ้นไป - เจ้าหน้าที่ดูหลักฐานแสดงตนและใช้เครื่องอ่านข้อมูลอิเล็กทรอนิกส์ หรือตรวจสอบแหล่งข้อมูลในรูปแบบอิเล็กทรอนิกส์จากหน่วยงานของรัฐแห่งอื่นเพื่อตรวจสอบว่าเป็นของแท้ - เจ้าหน้าที่เปรียบเทียบข้อมูลของผู้สมัครใช้บริการกับ

กลุ่มการให้บริการภาครัฐ	ระดับ IAL ขั้นต่ำ	ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน	พบเห็นต่อหน้า	ไม่พบเห็นต่อหน้า	เสมือนพบเห็นต่อหน้า
			ข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง		ข้อมูลอิเล็กทรอนิกส์จาก AS เพื่อตรวจสอบว่าข้อมูลมีความถูกต้อง
		การตรวจสอบตัวบุคคล	- เจ้าหน้าที่บันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (biometric sample) เช่น ภาพใบหน้า ลายนิ้วมือ - ใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)		- เจ้าหน้าที่บันทึกตัวอย่างข้อมูลชีวมิติของผู้สมัครใช้บริการ (biometric sample) เช่น ภาพใบหน้า ลายนิ้วมือ - ใช้เทคโนโลยีที่กำหนดเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของผู้สมัครใช้บริการกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison)
		การตรวจสอบช่องทางการติดต่อ	IdP <u>ต้อง</u>ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง เช่น หมายเลขโทรศัพท์เคลื่อนที่ อีเมล		IdP <u>ต้อง</u>ตรวจสอบช่องทางการติดต่อของผู้สมัครใช้บริการว่าสามารถใช้ติดต่อได้จริง เช่น หมายเลขโทรศัพท์เคลื่อนที่ อีเมล

การยืนยันตัวตนทางดิจิทัล (Authentication)

๓. ข้อกำหนดการยืนยันตัวตนทางดิจิทัล (Authentication Requirements)

ข้อกำหนดของการยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐ ให้เป็นไปตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน [๖] ข้อ ๒. ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (authenticator assurance level) โดยปัจจัยของการยืนยันตัวตน (authentication factor) มีรายละเอียดตามแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม ข้อ ๔.๓.๑ สิ่งที่ใช้ยืนยันตัวตน (authenticator)

๓.๑ 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 โดยที่ต้องเป็นรหัสผ่าน (something you know) ควบคู่กับการใช้ OTP ผ่านหมายเลขโทรศัพท์เคลื่อนที่ (something you have) โดยโพรโทคอลที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตนต้องเป็นโพรโทคอลที่มีความปลอดภัย เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงปานกลางถึงความเสี่ยงสูง

(๓) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ระดับที่ ๓ (AAL3)

กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบ ๒ ปัจจัยขึ้นไปที่แตกต่างกัน โดยมีปัจจัยหนึ่งเป็นกุญแจ (key) ที่ผ่านเกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol) ซึ่งผู้ใช้บริการต้องพิสูจน์ว่าตนครอบครองกุญแจนั้น และต้องพิสูจน์ว่าตนครอบครองปัจจัยของการยืนยันตัวตนดังกล่าวผ่านโพรโทคอลที่มีความปลอดภัยในการใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน และต้องมีการเข้ารหัสข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหว (sensitive data) รวมถึงสิ่งที่ใช้ยืนยันตัวตนเพื่อป้องกันการปลอมแปลง เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงสูง

๓.๒ ชนิดและข้อกำหนดสิ่งที่ใช้ยืนยันตัวตน (Authenticator and Verifier Requirements)

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

ทั้งนี้ การเปลี่ยนแปลงทางเทคโนโลยีหรือภัยคุกคาม อาจเกิดข้อจำกัดของสิ่งที่ใช้ยืนยันตัวตนที่ทำให้เสื่อมคุณภาพลง (restricted authenticator) โดยผู้พิสูจน์และยืนยันตัวตนต้องดำเนินการ ดังนี้

(๑) เสนอทางเลือกของสิ่งที่ใช้ยืนยันตัวตนที่ยังไม่เสื่อมคุณภาพและสอดคล้องกับข้อกำหนดของระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

(๒) จัดทำเอกสารแจ้งข้อมูล (notice) ให้ผู้ใช้บริการทราบถึงความเสี่ยงด้านความมั่นคงปลอดภัยของสิ่งที่ใช้ยืนยันตัวตนที่เสื่อมคุณภาพ รวมถึงทางเลือกของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้

(๓) ประเมินความเสี่ยงเกี่ยวกับสิ่งที่ใช้ยืนยันตัวตนที่อาจเสื่อมคุณภาพลงของผู้ใช้บริการเพิ่มเติม

(๔) จัดทำแผนการบรรเทาความเสี่ยงสิ่งที่ใช้ยืนยันตัวตนที่อาจเสื่อมคุณภาพ

๓.๓ การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน (Authenticator Lifecycle Management)

การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน ประกอบด้วยกระบวนการ ดังนี้

๓.๓.๑ การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน (Authenticator Binding)

การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน คือ การสร้างความสัมพันธ์ระหว่างสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตีของผู้ใช้บริการที่ออกโดยผู้พิสูจน์และยืนยันตัวตนในขั้นตอนของการลงทะเบียนเพื่อนำสิ่งที่ใช้ยืนยันตัวตนไปใช้ในการยืนยันตัวตนของผู้ใช้บริการ

โดยผู้พิสูจน์และยืนยันตัวตนดำเนินการ 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 โดยจัดส่งไปยังหมายเลขโทรศัพท์เคลื่อนที่หรืออีเมลของผู้สมัครใช้บริการ หรือใช้ข้อมูลชีวมิติที่ได้จัดเก็บไว้ตอนลงทะเบียนแบบพบเห็นต่อหน้าในการเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน

๓.๓.๒ การสูญหาย ถูกโจรกรรม และเสียหายของสิ่งที่ใช้ยืนยันตัวตน (Loss, Theft and Damage)

สิ่งที่ใช้ยืนยันตัวตนที่สูญหาย ถูกโจรกรรม หรือเสียหาย ถือว่าเป็นสิ่งที่ใช้ยืนยันตัวตนที่เสี่ยงต่อการใช้งานโดยผู้ไม่ประสงค์ดีในการนำสิ่งที่ใช้ยืนยันตัวตนไปใช้โดยไม่มีสิทธิ ดังนั้นผู้พิสูจน์และยืนยันตัวตน จึงควรให้ความสำคัญกับแนวปฏิบัติในกรณีสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกโจรกรรม และเสียหาย

โดยผู้พิสูจน์และยืนยันตัวตนดำเนินการ ดังนี้

(๑) ต้องจัดให้มีช่องทางสำหรับรายงานการสูญหาย ถูกโจรกรรม และเสียหายของสิ่งที่ใช้ยืนยันตัวตน

(๒) ควรจัดให้มีวิธีการยืนยันตัวตนสำรองหรือวิธีการอื่น ๆ ที่ใช้ตรวจสอบว่ารายงานการสูญหาย ถูกโจรกรรม และเสียหายของสิ่งที่ใช้ยืนยันตัวตน มาจากผู้ใช้บริการที่กล่าวอ้างจริง

(๓) ต้องระงับการใช้งาน เพิกถอน หรือทำลายสิ่งที่ใช้ยืนยันตัวตนทันที หลังจากตรวจพบว่าสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกโจรกรรม หรือเสียหาย

(๔) หลังจากสิ่งที่ใช้ยืนยันตัวตนถูกระงับการใช้งาน อาจมีการกำหนดระยะเวลาของการเปิดใช้งานใหม่อีกครั้ง หากเกินจากระยะเวลาที่กำหนดจะไม่สามารถกลับมาใช้งานได้อีก

(๕) ต้องดำเนินการพิสูจน์ตัวตนผู้ใช้บริการใหม่อีกครั้ง แต่ไม่จำต้องพิสูจน์ตัวตนใหม่ทั้งหมด ทั้งนี้ อาจตรวจสอบความสัมพันธ์ระหว่างตัวตนผู้ใช้บริการกับข้อมูลและหลักฐานแสดงตนที่ได้จัดเก็บไว้ในการลงทะเบียนและพิสูจน์ตัวตนไว้ก่อนหน้าด้วยวิธีการที่เหมาะสม

๓.๓.๓ การหมดอายุ (Expiration)

โดยผู้พิสูจน์และยืนยันตัวตนดำเนินการ ดังนี้

(๑) สิ่งที่ใช้ยืนยันตัวตนที่หมดอายุต้องไม่สามารถใช้ยืนยันตัวตนได้

(๒) เมื่อมีการยืนยันตัวตนโดยใช้สิ่งที่ใช้ยืนยันตัวตนที่หมดอายุ ควรแจ้งให้ผู้ใช้บริการทราบว่าการยืนยันตัวตนไม่สำเร็จเนื่องจากสิ่งที่ใช้ยืนยันตัวตนหมดอายุ

(๓) ควรเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนใหม่หรือต่ออายุการใช้งานสิ่งที่ใช้ยืนยันตัวตนในระยะเวลาที่เหมาะสมก่อนที่สิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการจะหมดอายุ

(๔) ต้องเพิกถอนหรือทำลายสิ่งที่ใช้ยืนยันตัวตนเดิม เมื่อผู้ใช้บริการได้รับและใช้สิ่งที่ใช้ยืนยันตัวตนใหม่

๓.๓.๔ การเพิกถอน (Revocation)

การเพิกถอนสิ่งที่ใช้ยืนยันตัวตน คือ การยุติความเชื่อมโยงระหว่างสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตีของผู้ใช้บริการ

โดยผู้พิสูจน์และยืนยันตัวตน ต้องเพิกถอนสิ่งที่ใช้ยืนยันตัวตนทันที เมื่อมีกรณีใดกรณีหนึ่ง ดังนี้

(๑) ไอเดนทิตีถูกเพิกถอน เช่น ผู้ใช้บริการเสียชีวิต ผู้ใช้บริการถูกตรวจพบว่ามีการหลอกลวงหรือปลอมแปลง หรือไม่แสดงตัวตนจริง

(๒) ผู้ใช้บริการต้องการเพิกถอนสิ่งที่ใช้ยืนยันตัวตนหรือยกเลิกการใช้บริการกับผู้พิสูจน์และยืนยันตัวตน

(๓) ในกรณีที่ตรวจพบในภายหลังว่าผู้ใช้บริการมีคุณสมบัติไม่ตรงตามเกณฑ์ที่ผู้พิสูจน์และยืนยันตัวตนกำหนด

๓.๔ การบริหารจัดการเซสชัน (Session Management)

การกำหนดเซสชัน อาจเริ่มตั้งแต่การยืนยันตัวตนไปจนถึงการสิ้นสุดการใช้งาน ทั้งนี้ การยกเลิกเซสชัน อาจเกิดขึ้นได้ เช่น การไม่มีกิจกรรมใด ๆ เกิดขึ้นในระยะเวลาที่กำหนด หรือถูกยกเลิกโดยผู้ใช้บริการ หากต้องการใช้บริการต่อจากเซสชันเดิมที่ถูกยกเลิกแล้ว ให้ผู้ใช้บริการยืนยันตัวตนซ้ำอีกครั้งเพื่อเข้าใช้งาน

๓.๔.๑ 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) ไม่ควรจัดเก็บเซสชันไว้ในสถานที่ที่ไม่ปลอดภัย เช่น HTML5 ซึ่งอาจเสี่ยงต่อการโจมตีแบบ cross-site scripting (XSS)

(๖) ต้องส่งและรับเซสชันจากอุปกรณ์ผ่านช่องทางที่มีความปลอดภัย

(๗) ต้องตั้งเวลาหมดอายุ ไม่ให้ใช้งานได้ ดังนี้

(๗.๑) ๓๐ วัน สำหรับ AAL1

(๗.๒) ๑๒ ชั่วโมง หรือ ๓๐ นาทีหากไม่มีกิจกรรมใด ๆ เกิดขึ้น สำหรับ AAL2

(๗.๓) ๑๒ ชั่วโมง หรือ ๑๕ นาทีหากไม่มีกิจกรรมใด ๆ เกิดขึ้น สำหรับ AAL3

(๘) ต้องไม่สามารถใช้งานผ่านช่องทางการสื่อสารที่ไม่ปลอดภัย และเมื่อยืนยันตัวตนสำเร็จต้องไม่ลดระดับไปยังช่องทางการสื่อสารที่ไม่ปลอดภัย เช่น จาก HTTPS เป็น HTTP

๓.๔.๑.๑ เบราว์เซอร์คุกกี้ (Browser Cookies)

เบราว์เซอร์คุกกี้เป็นกลไกที่ใช้สำหรับสร้างเซสชัน และติดตามผู้ใช้บริการขณะที่เข้าใช้บริการ ควรกำหนดดังนี้

(๑) ต้องกำหนดให้มีการเข้าถึงคุกกี้ได้เฉพาะการเชื่อมต่อที่ใช้งาน HTTPS เท่านั้น

(๒) ต้องระบุ hostname และ path ที่อนุญาตให้ใช้คุกกี้น้อยที่สุดเท่าที่จำเป็น

(๓) ควรกำหนดให้ JavaScript ไม่สามารถเข้าถึงคุกกี้ได้ โดยการกำหนด flag HttpOnly ให้กับคุกกี้

(๔) ควรกำหนดระยะเวลาหมดอายุของคุกกี้

๓.๔.๑.๒ แอกเซสโทเค็น (Access Token)

แอกเซสโทเค็นใช้สำหรับอนุญาตให้แอปพลิเคชันเข้าถึงบริการภาครัฐในฐานะของผู้ใช้บริการหลังจากการยืนยันตัวตนสำเร็จ โดยผู้ให้บริการภาครัฐต้องไม่ถือว่าการแสดง OAuth access token เป็นการยืนยันตัวตนตามหลักการของดิจิทัลไอดี ซึ่งอาจใช้องค์ประกอบอื่น ๆ เพิ่มเติมด้วย เนื่องจาก OAuth access token และ refresh token ที่เกี่ยวข้อง อาจคงสถานะการใช้งานได้หลังจากการสิ้นสุดเซสชันและผู้ใช้บริการได้ออกจากแอปพลิเคชันไปแล้ว

๓.๔.๑.๓ การระบุอุปกรณ์ (Device Identification)

วิธีการระบุอุปกรณ์ที่มีความปลอดภัย เช่น การใช้โพรโทคอล TLS หรือการเชื่อมโยงโทเค็น (token binding) หรือวิธีการอื่น ๆ อาจนำมาใช้สร้างเซสชันระหว่างผู้ใช้บริการกับบริการภาครัฐได้

๓.๔.๒ การยืนยันตัวตนซ้ำ (Reauthentication)

ความต่อเนื่องของเซสชันต้องขึ้นอยู่กับความลับของเซสชันที่ครอบครองในช่วงเวลาของการยืนยันตัวตนที่ออกโดยผู้พิสูจน์และยืนยันตัวตน และอาจมีการ refresh session

ความลับของเซสชันต้องไม่คงอยู่ถาวรและต้องไม่เก็บไว้หากมีการเริ่มใช้งาน (restart) แอปพลิเคชันใหม่ หรือรีบูต (reboot) เครื่องที่ให้บริการ

การยืนยันตัวตนซ้ำตามช่วงเวลาที่กำหนดของแต่ละระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ต้องเกิดขึ้นเพื่อยืนยันว่าผู้ใช้บริการยังคงมีสถานะใช้งานอยู่ ก่อนที่เซสชัน

จะสิ้นสุดเนื่องจากหมดเวลาหรือด้วยเหตุผลอื่น ๆ ผู้ใช้บริการต้องยืนยันตัวตนซ้ำเพื่อต่ออายุการใช้งานเซสชันโดยมีวิธีการ ดังนี้

(๑) ระดับ AAL1 : ยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนอย่างน้อยหนึ่งปัจจัย

(๒) ระดับ AAL2 : ยืนยันตัวตนโดยใช้รหัสลับจดจำหรือชีวมิติ

(๓) ระดับ AAL3 : ยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนทั้งหมด

เมื่อถึงเวลาที่กำหนดไว้ เซสชันควรถูกทำให้สิ้นสุดลง (terminated) เช่น การออกจากระบบ ทั้งนี้ เมื่อเซสชันถูกทำให้สิ้นสุดลงแล้ว ผู้ใช้บริการจะต้องยืนยันตัวตนใหม่อีกครั้งโดยต้องมีการสร้างเซสชันใหม่ขึ้นมา

๓.๕ ภัยคุกคาม (Threats and Security Considerations)

นอกจากนี้ ในกระบวนการยืนยันตัวตนต้องคำนึงถึงภัยคุกคามที่อาจจะก่อให้เกิดความเสียหายแก่ระบบงานและข้อมูลต่าง ๆ ขึ้นได้ ดังนี้

ตารางที่ ๓ ภัยคุกคามและการบรรเทาภัยคุกคามที่อาจเกิดขึ้นในขั้นตอนการยืนยันตัวตน

ภัยคุกคาม	รายละเอียด	ตัวอย่าง	การบรรเทาภัยคุกคามที่อาจเกิดขึ้น
การเดาออนไลน์ (online guessing)	เป็นวิธีการที่ผู้ไม่ประสงค์ดีพยายามเข้าระบบ (login) ซ้ำ ๆ โดยทดลองเดาผลลัพธ์หรือค่าต่าง ๆ ที่จะสามารถผ่านเข้าไปยังระบบได้	การพยายามเข้าเว็บไซต์โดยลักลอบใช้ชื่อผู้ใช้งาน (username) และทดลองใช้รหัสผ่าน (password) ที่ผู้ใช้บริการอาจใช้บ่อย ๆ	ป้องกันไม่ให้ผู้ไม่ประสงค์ดีล่วงรู้หรือคาดเดาข้อมูลเฉพาะของผู้ใช้บริการที่ใช้เป็นข้อมูลลับในการยืนยันตัวตน โดย IdP ควรคำนึงถึงระดับความยากง่ายของการสร้างข้อมูลลับ ความปลอดภัยของข้อมูลที่รับส่งผ่านช่องทางการยืนยันตัวตน และวิธีการบริหารจัดการอื่น ๆ เช่น การใช้รหัสผ่านที่คาดเดายาก และจำกัดจำนวนครั้งของความพยายามในการยืนยันตัวตนที่ไม่สำเร็จ หากครบจำนวนแล้วต้องกำหนดระยะเวลาที่สามารถเข้าสู่ระบบได้ใหม่ในครั้งถัดไป
การส่งข้อมูลซ้ำ (replay attack)	เป็นวิธีการที่ผู้ไม่ประสงค์ดีสามารถนำข้อมูลที่เคยดักจับได้กลับมาใช้ยืนยันตัวตนเพื่อเข้าระบบเสมือนเป็นผู้ใช้บริการ	ผู้ไม่ประสงค์ดีอาจดักจับรหัสผ่านจากผู้ใช้บริการในขณะยืนยันตัวตน และนำรหัสผ่านนั้นมาเข้าระบบในภายหลัง	ใช้ช่องทางการสื่อสารที่มีการตรวจสอบความเป็นปัจจุบัน หรือมีการจำกัดเวลาของการใช้งานที่สอดคล้องกับช่วงเวลาในการยืนยันตัวตนในปัจจุบัน
การขโมยเซสชัน (session hijack)	เป็นวิธีการที่ผู้ไม่ประสงค์ดีสามารถเข้าควบคุมเซสชัน ซึ่งอาจจะเป็นการแฝงตัวในการสื่อสารที่แลกเปลี่ยนข้อมูลการยืนยันตัวตนระหว่างผู้ใช้บริการและ IdP เพื่อเข้าควบคุมการสื่อสารนั้นไว้	ผู้ไม่ประสงค์ดีสามารถเข้าควบคุมการสื่อสารที่แลกเปลี่ยนข้อมูลการยืนยันตัวตน แล้วดักจับข้อมูลหรือคาดเดาค่า (value) ของคุกกี้ที่ใช้ในการยืนยันตัวตน (authentication cookies) เพื่อระบุ HTTP requests ของผู้ใช้บริการ	ใช้ช่องทางสื่อสารในการยืนยันตัวตนระหว่างผู้ใช้บริการและ IdP ที่มีการควบคุมการรับส่งข้อมูลต่อช่วงเวลา (per-session data transfer protocol)

ภัยคุกคาม	รายละเอียด	ตัวอย่าง	การบรรเทาภัยคุกคามที่อาจเกิดขึ้น
การแอบดักจับข้อมูล (eavesdropping)	เป็นวิธีการที่ผู้ไม่ประสงค์ดีลักลอบดักจับข้อมูลจากช่องทางการสื่อสาร เพื่อนำข้อมูลที่ได้ไปใช้ปลอมแปลงเป็นผู้ใช้บริการในการยืนยันตัวตนเข้าระบบ	แอบส่องรหัสลับจดจำเมื่อผู้ใช้งานพิมพ์รหัสลงบนแป้นพิมพ์ หรือใช้ซอฟต์แวร์ดักจับข้อมูลที่ได้มีการบันทึกการพิมพ์รหัสลงบนแป้นพิมพ์ (keystroke)	ป้องกันไม่ให้ผู้ไม่ประสงค์ดีล่วงรู้ข้อมูลเฉพาะของผู้ใช้บริการ ที่ใช้เป็นข้อมูลลับในการยืนยันตัวตนโดยใช้ช่องทางการสื่อสารที่ป้องกันการดักจับข้อมูล รวมถึงควรมีมาตรการมิให้บุคคลอื่นที่ทำการดักจับข้อมูลสามารถนำข้อมูลไปใช้ได้ เช่น transport layer security (TLS) protocol
การหลอกลวง (phishing)	เป็นวิธีการที่ผู้ใช้บริการถูกล่อลวงโดยผู้ไม่ประสงค์ดี เพื่อให้เปิดเผยข้อมูลลับ ข้อมูลส่วนตัว หรือข้อมูลที่ใช้ในการยืนยันตัวตน โดยผู้ไม่ประสงค์ดีจะนำข้อมูลต่าง ๆ ที่ได้ไปปลอมตัวเป็นผู้ใช้บริการ เพื่อยืนยันตัวตนเข้าใช้บริการภาครัฐ	การส่งอีเมลเพื่อล่อลวงให้ผู้ใช้บริการเข้าไปยังเว็บไซต์ที่ผู้ไม่ประสงค์ดีทำปลอมขึ้นมา โดยทำให้ผู้ใช้บริการคิดว่าเป็นเว็บไซต์จริง และล่อลวงให้ใส่ชื่อผู้ใช้งานและรหัสผ่านเพื่อเข้าระบบ เช่น เว็บไซต์ของ IdP ที่ผู้ใช้บริการมีบัญชี (account) อยู่	ป้องกันไม่ให้ผู้ไม่ประสงค์ดีสามารถล่วงรู้หรือเรียนรู้ข้อมูลและพฤติกรรมส่วนตัวของผู้ใช้บริการ รวมถึงสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ
การลักลอบเป็นคนกลาง (man-in-the-middle)	เป็นวิธีการที่ผู้ไม่ประสงค์ดีแฝงตัวอยู่ในช่องทางการสื่อสารเพื่อลักลอบ ขัดขวาง แก้ไข หรือใช้เนื้อหาข้อมูลที่แลกเปลี่ยนกันในการยืนยันตัวตนระหว่างผู้ใช้บริการและ IdP เพื่อให้ผู้ไม่ประสงค์ดีสามารถเข้าระบบได้ โดยปกติแล้วผู้ไม่ประสงค์ดีจะปลอมตัวเป็น IdP เพื่อหลอกผู้ใช้บริการ และในทำนองเดียวกันก็สามารถปลอมตัวเป็นผู้ใช้บริการเพื่อหลอก IdP ตัวตนได้เช่นกัน	ถ้าผู้ใช้บริการต้องการส่งข้อมูลไปยัง IdP โดยมีการเข้ารหัสข้อมูลด้วยกุญแจสาธารณะของ IdP ในช่องทางการสื่อสาร ผู้ไม่ประสงค์ดีจะทำการสับเปลี่ยนกุญแจสาธารณะโดยส่งกุญแจสาธารณะของผู้ไม่ประสงค์ดีไปให้ผู้ใช้บริการและล่อลวงให้เข้ารหัสด้วยกุญแจสาธารณะนั้นแทน ซึ่งผู้ไม่ประสงค์ดีจะสามารถถอดรหัสข้อมูลนั้นได้ด้วยกุญแจส่วนตัวของผู้ไม่ประสงค์ดี	ตรวจสอบกระบวนการยืนยันตัวตน ให้แน่ใจว่าข้อมูลที่ถูกส่งระหว่างกันไม่สามารถดักจับได้ หากมีการส่งความลับ (secret) หรือข้อมูลส่วนตัวผ่านทางอินเทอร์เน็ตต้องทำการเข้ารหัสก่อนทุกครั้ง ควรใช้เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (PKI) ในการยืนยันตัวตนระหว่างฝั่งของผู้ใช้บริการและฝั่งของ IdP หรือใช้ช่องทางที่อนุญาตให้ผู้ใช้บริการเปิดเผยความลับไปยัง IdP ตัวจริงเท่านั้น

๓.๖ ข้อกำหนดขั้นต่ำในการยืนยันตัวตนทางดิจิทัล (Minimum Requirement of Authentication)

เมื่อผู้ใช้บริการลงทะเบียนและพิสูจน์ตัวตน และได้รับสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ในการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตนเรียบร้อยแล้ว หากผู้ใช้บริการต้องการเข้าใช้บริการออนไลน์กับผู้ให้บริการภาครัฐและผู้ให้บริการภาครัฐต้องการทราบว่าผู้ใช้บริการเป็นผู้ใด

สำหรับผู้ใช้บริการที่เคยลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตนที่ผู้ให้บริการภาครัฐเชื่อถือ ผู้ให้บริการภาครัฐจะนำผู้ใช้บริการไปยังหน้าต่างยืนยันตัวตนของผู้พิสูจน์และยืนยันตัวตนนั้น ผู้ใช้บริการต้องยืนยันตัวตนด้วยการพิสูจน์ให้เห็นว่าตนครอบครองสิ่งที่ใช้ยืนยันตัวตนตามเกณฑ์วิธีที่ผู้พิสูจน์และยืนยันตัวตนกำหนด เมื่อตรวจสอบสิ่งที่ใช้ยืนยันตัวตนและสิ่งที่ใช้รับรองตัวตนเรียบร้อยแล้ว ผู้พิสูจน์และยืนยันตัวตนจะส่งผลการยืนยันตัวตนให้กับผู้ให้บริการภาครัฐ เพื่อให้ผู้ให้บริการภาครัฐนำไปใช้พิจารณาอนุญาตเข้าใช้บริการภาครัฐต่อไป

ข้อกำหนดขั้นต่ำในการยืนยันตัวตนทางดิจิทัล จำแนกตามกลุ่มการให้บริการภาครัฐ ดังนี้

(๑) กลุ่มการให้บริการข้อมูลพื้นฐาน จัดเป็นบริการที่ไม่มีความเสี่ยงหรือมีความเสี่ยงต่ำ จึง**ไม่จำเป็นต้องใช้ดิจิทัลไอดี**

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

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

(๔) กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงานที่มีความเสี่ยงสูง 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 AAL๒ และ AAL๓
		การยืนยันตัวตนซ้ำ	อย่างน้อยทุก ๓๐ วัน
		การป้องกันการโจมตีโดยคนกลางของช่องทางที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน	จำเป็น
		การป้องกันการโจมตีแบบส่งข้อมูลซ้ำของสิ่งที่ใช้ยืนยันตัวตน	ไม่จำเป็น
		การป้องกันผู้พิสูจน์และยืนยันตัวตนปลอมของสิ่งที่ใช้ยืนยันตัวตน	ไม่จำเป็น

กลุ่มการให้บริการภาครัฐ	ระดับ AAL ขั้นต่ำ	การยืนยันตัวตน	ข้อกำหนด
- **กลุ่มการให้บริการธุรกรรม** - **กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงานที่มีความเสี่ยงสูง**	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 AAL๓
		การยืนยันตัวตนซ้ำ	- อย่างน้อยทุก ๑๒ ชั่วโมง **หรือ** - ๓๐ นาทีหากไม่มีกิจกรรมใด ๆ เกิดขึ้น ผู้ใช้บริการอาจยืนยันตัวตนโดยใช้ ๑ ปัจจัย (รหัสลับจดจำหรือชีวมิติ)
		การป้องกันการโจมตีโดยคนกลางของช่องทางที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน	จำเป็น

กลุ่มการให้บริการภาครัฐ	ระดับ AAL ขั้นต่ำ	การยืนยันตัวตน	ข้อกำหนด
		การป้องกันการโจมตีแบบส่งข้อมูลซ้ำของสิ่งที่ใช้ยืนยันตัวตน	จำเป็น
		การป้องกันผู้พิสูจน์และยืนยันตัวตนปลอมของสิ่งที่ใช้ยืนยันตัวตน	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)

กลุ่มการให้บริการภาครัฐ	ระดับ AAL ขั้นต่ำ	การยืนยันตัวตน	ข้อกำหนด
		การยืนยันตัวตนซ้ำ	- อย่างน้อยทุก ๑๒ ชั่วโมง **หรือ** - ๑๕ นาทีหากไม่มีกิจกรรมใด ๆ เกิดขึ้น ผู้ใช้บริการต้องยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนทั้งหมด
		การป้องกันการโจมตีโดยคนกลางของช่องทางที่ใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน	จำเป็น
		การป้องกันการโจมตีแบบส่งข้อมูลซ้ำของสิ่งที่ใช้ยืนยันตัวตน	จำเป็น
		การป้องกันผู้พิสูจน์และยืนยันตัวตนปลอมของสิ่งที่ใช้ยืนยันตัวตน	จำเป็น

๔. การพิจารณาการคุ้มครองข้อมูลส่วนบุคคล (Privacy Considerations)

การพิจารณาการคุ้มครองข้อมูลส่วนบุคคล ควรพิจารณาดังนี้

๔.๑ การจัดเก็บข้อมูลเท่าที่จำเป็น (Data Minimization)

ตามพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๒๒ กำหนดให้มีการเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล โดยต้องมีแนวทางในการดำเนินการเพื่อประกันการจัดเก็บข้อมูลเท่าที่จำเป็นทั้งในแง่ของประเภทข้อมูลและระยะเวลาการจัดเก็บข้อมูล ซึ่งการจัดเก็บข้อมูลเท่าที่จำเป็นจะเป็นการลดความเสี่ยงที่อาจเกิดขึ้นได้จากการใช้งานหรือเข้าถึงโดยไม่ได้รับอนุญาต

ทั้งนี้ ในการจัดเก็บข้อมูลส่วนบุคคล ผู้พิสูจน์และยืนยันตัวตนควรพิจารณาถึงการดำเนินการคุ้มครองข้อมูลส่วนบุคคล ให้สอดคล้องกับกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลเป็นสำคัญ

๔.๒ เอกสารแจ้งข้อมูลและเอกสารแสดงความยินยอม (Privacy Notice and Consent)

ตามพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๑๙ ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้พิสูจน์และยืนยันตัวตนต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่ายและไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว

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

ในกรณีถอนความยินยอมผู้พิสูจน์และยืนยันตัวตนต้องแจ้งส่งผลกระทบจากการถอนความยินยอมให้เจ้าของข้อมูลส่วนบุคคลทราบ ทั้งนี้ การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลที่ไม่เป็นไปตามที่กฎหมายกำหนด จะไม่มีผลผูกพันกับเจ้าของข้อมูลส่วนบุคคล และผู้พิสูจน์และยืนยันตัวตนไม่สามารถเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้

๔.๓ การคุ้มครองความเป็นส่วนบุคคล (Privacy Control)

ผู้พิสูจน์และยืนยันตัวตนควรจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยด้านการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม โดยครอบคลุมถึงการแจ้งเตือน การแก้ไข หรือการพิจารณาอื่น ๆ ที่สำคัญ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม รวมถึงการขอความยินยอมต้องทำเป็นลายลักษณ์อักษรที่ชัดเจน และทำผ่านระบบอิเล็กทรอนิกส์ได้

๔.๔ 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

๔.๕ การแก้ไขข้อมูลส่วนบุคคล (Redress)

ผู้พิสูจน์และยืนยันตัวตนต้องจัดให้มีกลไกสำหรับการแก้ไขข้อมูลตามข้อร้องเรียนหรือปัญหาของผู้สมัครใช้บริการที่เกิดขึ้นจากการพิสูจน์ตัวตน โดยกลไกดังกล่าวต้องให้ผู้สมัครใช้บริการค้นหาและใช้งานได้ง่าย ทั้งนี้ควรจัดให้มีวิธีการอื่น ๆ เช่น วิธีการแบบพบเห็นต่อหน้า เพื่อรองรับในกรณีที่ผู้สมัครใช้บริการไม่สามารถแก้ไขข้อมูลได้ด้วยวิธีการแบบออนไลน์

๔.๖ การประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล (Privacy Risk Assessment)

ผู้พิสูจน์และยืนยันตัวตน ควรพิจารณาดังนี้

(๑) โอกาสที่จะเกิดการดำเนินงานที่สร้างหรือก่อให้เกิดปัญหาต่อผู้สมัครใช้บริการหรือผู้ใช้บริการในระบบ เช่น ขั้นตอนการตรวจสอบหรือการจัดเก็บบันทึกข้อมูลส่วนบุคคลอาจทำให้เกิดการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

(๒) ผลกระทบเมื่อเกิดปัญหาขึ้น

ผู้พิสูจน์และยืนยันตัวตนควรมีแนวทางในการตอบสนองต่อความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลที่รวมถึงการยอมรับความเสี่ยง การบรรเทาความเสี่ยง และการแบ่งปันความเสี่ยง ทั้งนี้ การให้ความยินยอมของผู้ใช้บริการถือเป็นรูปแบบหนึ่งของการแบ่งปันความเสี่ยง ซึ่งใช้ได้เฉพาะกับผู้ใช้บริการที่ยอมรับข้อตกลงและเงื่อนไขการให้บริการที่เหมาะสมเพียงพอที่จะแบ่งปันความเสี่ยงได้

๔.๗ การดำเนินการให้สอดคล้องกับการคุ้มครองข้อมูลส่วนบุคคล (Privacy Compliance)

ผู้พิสูจน์และยืนยันตัวตนควรพิจารณาถึงการดำเนินการให้สอดคล้องกับการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดไว้ เช่น กฎหมาย ข้อกำหนด ข้อตกลง นโยบาย แนวปฏิบัติ เพื่อที่จะประเมินและบรรเทาความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล รวมถึงการให้คำแนะนำกับหน่วยงานที่เกี่ยวข้องเพื่อปฏิบัติ

๕. แนวทางการนำไปใช้ (Usability Considerations)

ในการพิสูจน์และยืนยันตัวตนทางดิจิทัลสามารถกำหนดข้อตกลงร่วมกันในการพิสูจน์และยืนยันตัวตนทางดิจิทัลระหว่างผู้พิสูจน์และยืนยันตัวตน ผู้ให้บริการภาครัฐ และแหล่งให้ข้อมูลที่น่าเชื่อถือ ดังนี้

๕.๑ สำหรับผู้พิสูจน์และยืนยันตัวตน (Identity Provider: IdP)

๕.๑.๑ กำหนดรูปแบบของการพิสูจน์และยืนยันตัวตนทางดิจิทัลให้สอดคล้องกับระดับความน่าเชื่อถือ

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

๕.๑.๒ กำหนดนโยบายและกระบวนการปฏิบัติงานภายในที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ชัดเจนเป็นลายลักษณ์อักษร

ต้องทบทวน สื่อสาร ทำความเข้าใจ สร้างความตระหนักให้กับเจ้าหน้าที่ที่ได้รับการฝึกอบรมหรือบุคลากรที่เกี่ยวข้องให้เห็นถึงความสำคัญ และปฏิบัติตามนโยบายและกระบวนการปฏิบัติงานภายในหรือหน่วยงานกำกับดูแลที่เกี่ยวข้อง รวมถึงต้องสื่อสารทำความเข้าใจและให้ความรู้กับผู้ใช้บริการด้วย

๕.๑.๓ ดำเนินการตามข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลตามกลุ่มการให้บริการภาครัฐ

กรณีที่ผู้พิสูจน์และยืนยันตัวตนเป็นหน่วยงานของรัฐต้องดำเนินการตามข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล รายละเอียดตามข้อ ๒. ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล ดังนี้

(๑) รวบรวมข้อมูลเพื่อระบุตัวตน

(๒) ตรวจสอบหลักฐานแสดงตน

(๓) ตรวจสอบตัวบุคคล

ทั้งนี้ หากผู้พิสูจน์และยืนยันตัวตนเป็นหน่วยงานของเอกชนให้ดำเนินการตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๕.๑.๔ ดำเนินการตามข้อกำหนดการยืนยันตัวตนทางดิจิทัลตามกลุ่มการให้บริการภาครัฐ

ต้องดำเนินการตามข้อกำหนดของการยืนยันตัวตนทางดิจิทัล รายละเอียดตามข้อ ๓. ข้อกำหนดการยืนยันตัวตนทางดิจิทัล

ทั้งนี้ต้องพิจารณาถึงการคุ้มครองข้อมูลส่วนบุคคล รายละเอียดตามข้อ ๔.

๕.๑.๕ ต้องจัดให้มีการขอความยินยอมของผู้สมัครใช้บริการ

โดยต้องแจ้งวัตถุประสงค์ของการจัดเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลด้วย

๕.๑.๖ ต้องจัดให้มีการแสดงตนและรวบรวมข้อมูลเพื่อระบุตัวตนที่จำเป็นจากผู้สมัครใช้บริการ

เพื่อแยกแยะว่าไอเดนทิตีของผู้สมัครใช้บริการมีเพียงหนึ่งเดียว และมีความเฉพาะเจาะจงภายในบริบทของผู้ใช้บริการทั้งหมดที่ผู้พิสูจน์และยืนยันตัวตนดูแล

๕.๑.๗ ต้องเก็บรักษาข้อมูลและหลักฐานแสดงตน

รวมถึงภาพและเสียง (ถ้ามี) และการบันทึกเหตุการณ์และรายละเอียดการทำธุรกรรมเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยระยะเวลาการเก็บรักษาและการบันทึกดังกล่าวให้เป็นไปตามกฎหมาย ข้อบังคับ หรือแนวนโยบายที่เกี่ยวข้อง

๕.๑.๘ ดำเนินการตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนดตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๕.๑.๙ ประกาศข้อกำหนดให้ผู้ที่เกี่ยวข้องในกระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัลทราบโดยทั่วกัน

๕.๒ สำหรับผู้ให้บริการภาครัฐ

การเลือกใช้รูปแบบ วิธีการ รวมถึงระดับความน่าเชื่อถือที่เหมาะสมกับบริการภาครัฐนั้น มีความสำคัญอย่างยิ่ง ดังนั้นการออกแบบและการนำไปใช้ ต้องคำนึงถึงกระบวนการ [๗] ดังนี้

๕.๒.๑ กำหนดความต้องการและระบบของหน่วยงานของรัฐที่ต้องการใช้ดิจิทัลไอดี

ต้องกำหนดความต้องการและระบบของบริการภาครัฐของหน่วยงานของตนที่ต้องการใช้ดิจิทัลไอดี ทั้งนี้ ผลลัพธ์ที่ได้จะนำไปใช้ในการวิเคราะห์และประเมินความเสี่ยง โดยพิจารณาดังนี้

(๑) กำหนดบริการภาครัฐอย่างชัดเจนว่ามีบริการใดบ้างที่จำเป็นต้องใช้ข้อมูลส่วนบุคคลในการให้บริการ
(๒) กำหนดบริการภาครัฐอย่างชัดเจนว่าจำเป็นต้องลงทะเบียนและพิสูจน์ตัวตนหรือไม่
(๓) กำหนดผู้เกี่ยวข้อง บทบาท และหน้าที่
(๔) กำหนดช่องทางดิจิทัลที่ใช้ในการรับส่งข้อมูล เช่น อีเมล หมายเลขโทรศัพท์เคลื่อนที่

๕.๒.๒ ประเมินความเสี่ยง

ต้องพิจารณาถึงผลกระทบ ระดับความรุนแรง และความสูญเสียที่อาจเกิดขึ้นได้หากการพิสูจน์และยืนยันตัวตนผิดพลาด และควรมุ่งเน้นที่กระบวนการธุรกรรมออนไลน์เป็นหลัก รายละเอียดตามแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม ข้อ ๖.๓ ความเสี่ยงและผลกระทบ

๕.๒.๓ กำหนดระดับความน่าเชื่อถือ

ต้องนำผลการจัดระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือของไอเดนทิตีเมื่อเกิดข้อผิดพลาดในการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลจากข้อ ๕.๒.๒ มาใช้พิจารณาระดับความน่าเชื่อถือของไอเดนทิตี รายละเอียดตามแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม ข้อ ๗. การกำหนดระดับความน่าเชื่อถือของไอเดนทิตี

และต้องนำผลการจัดระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนเมื่อเกิดข้อผิดพลาดในการยืนยันตัวตนทางดิจิทัลจากข้อ ๕.๒.๒ มาใช้พิจารณาระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน รายละเอียดตามแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม ข้อ ๘. การกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

๕.๒.๔ เลือกรูปแบบ และวิธีการลงทะเบียน พิสูจน์ตัวตน และยืนยันตัวตนทางดิจิทัล

พิจารณาจัดรูปแบบการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลสำหรับบริการภาครัฐ โดยผู้พิสูจน์และยืนยันตัวตนจะเป็นผู้รับผิดชอบดูแลเกี่ยวกับการรับลงทะเบียน การพิสูจน์ตัวตน และบริหารจัดการสิ่งที่ใช้รับรองตัวตน ซึ่งเชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ โดยต้องมีการรวบรวมข้อมูลเพื่อระบุตัวตน การตรวจสอบหลักฐานแสดงตน การตรวจสอบตัวบุคคล หรือการตรวจสอบช่องทางการติดต่อ ตามแต่ละระดับความน่าเชื่อถือเพื่อกำหนดวิธีการลงทะเบียน รายละเอียดตามข้อ ๒. ข้อกำหนดการลงทะเบียนและพิสูจน์ตัวตน

ทางดิจิทัล รวมถึงเลือกปัจจัยและชนิดของสิ่งที่ใช้ยืนยันตัวตนที่เหมาะสม รายละเอียดตามข้อ ๓. ข้อกำหนดการยืนยันตัวตนทางดิจิทัล

๕.๒.๕ ทบทวนความถูกต้องเหมาะสม

ต้องทบทวนถึงองค์ประกอบและความพร้อมทั้งหมดก่อนดำเนินการในกระบวนการพิสูจน์และยืนยันตัวตน นอกจากนี้ควรจะพิจารณาในเรื่องของค่าใช้จ่ายและผลประโยชน์ก่อนตัดสินใจดำเนินการต่าง ๆ รวมถึงควรประเมินระบบและเทคโนโลยีที่ใช้ในการพิสูจน์และยืนยันตัวตนเป็นประจำ

๕.๓ สำหรับแหล่งให้ข้อมูลที่น่าเชื่อถือ (Authoritative Source: AS)

๕.๓.๑ ตรวจสอบข้อมูลหรือสถานะของหลักฐานแสดงตนของผู้สมัครใช้บริการ

เมื่อผู้สมัครใช้บริการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล แหล่งให้ข้อมูลที่น่าเชื่อถือจะตรวจสอบข้อมูลหรือสถานะของหลักฐานแสดงตนของผู้สมัครใช้บริการตามการร้องขอจากผู้พิสูจน์และยืนยันตัวตน และส่งผลการตรวจสอบข้อมูลกลับไปยังผู้พิสูจน์และยืนยันตัวตน

ทั้งนี้ หากบริการภาครัฐใดที่ต้องใช้ข้อมูลส่วนบุคคลในการพิสูจน์และยืนยันตัวตนทางดิจิทัล ให้กำหนดระดับความน่าเชื่อถือของไอเดนทิตีขั้นต่ำที่ระดับ ๒ ซึ่งเทียบเท่ากับระดับความน่าเชื่อถือของไอเดนทิตีที่ระดับ ๒.๑ ของประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย - การลงทะเบียนและพิสูจน์ตัวตน เมื่อครบระยะเวลาดังกล่าว

บรรณานุกรม

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

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

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

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

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

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

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

[๘] Department of Economic and Social Affairs. (2012). *United Nations E-Government Survey ๒๐๑๒.* United Nations, New York.

[๙] ธนาคารแห่งประเทศไทย. (๒๕๖๒). *หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน*. ประกาศธนาคารแห่งประเทศไทย ที่ สนส. ๑๙/๒๕๖๒ ประกาศ ณ วันที่ ๒๓ สิงหาคม ๒๕๖๒ คัดจากราชกิจจานุเบกษา เล่มที่ ๑๓๖ ตอนพิเศษ ๒๑๙ ง วันที่ ๒ กันยายน ๒๕๖๒.

[๑๐] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (๒๕๖๑). *ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทำธุรกรรมแบบพบเห็นลูกค้าต่อหน้าสำหรับธนาคาร*. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.