สพร. / CDV
สิงหาคม ๒๕๖๓

มาตรฐานรัฐบาลดิจิทัลอยู่ระหว่างการจัดทำ
ห้ามใช้หรือยึดร่างนี้เป็นมาตรฐาน

มาตรฐานรัฐบาลดิจิทัลฉบับสมบูรณ์จะมีประกาศโดย
คณะกรรมการพัฒนารัฐบาลดิจิทัล

ร่าง

มาตรฐานรัฐบาลดิจิทัล
Digital Government Standard

ว่าด้วย แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม

DIGITALIZATION: DIGITAL ID - OVERVIEW

สำหรับเวียนขอข้อคิดเห็นจากหน่วยงานต่าง ๆ ที่เกี่ยวข้อง

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

สารบัญ

สารบัญตาราง

สารบัญภาพ

คำนำ

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

การพิสูจน์และยืนยันตัวตนทางดิจิทัล เป็นกระบวนการแรกที่สำคัญในการเข้าสู่บริการต่าง ๆ ของภาครัฐ ซึ่งหน่วยงานของรัฐต้องประเมินความต้องการของหน่วยงานเพื่อพิจารณาว่าบริการใดบ้างที่จำเป็นต้องใช้ดิจิทัลไอดีในการพิสูจน์และยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐ โดยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ ประกอบด้วย

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

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

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

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

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

แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม

๑. ที่มา เหตุผล และความจำเป็น

ตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ มีวัตถุประสงค์เพื่อให้การบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน ให้หน่วยงานของรัฐจัดให้มีการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัล โดยมีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคง ปลอดภัยและมีธรรมาภิบาล

เพื่อให้การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัลเป็นไปตามวัตถุประสงค์ดังกล่าวข้างต้น โดยที่มาตรา ๑๒ (๒) กำหนดให้หน่วยงานของรัฐจัดทำกระบวนการหรือการดำเนินงานทางดิจิทัลเพื่อการบริหารราชการแผ่นดินและการให้บริการประชาชน กระบวนการหรือการดำเนินงานทางดิจิทัลนั้นต้องทำงานร่วมกันได้ตามมาตรฐาน ข้อกำหนด และหลักเกณฑ์ที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด เพื่อให้มีความสอดคล้องและเชื่อมโยงระหว่างหน่วยงานของรัฐแห่งอื่นได้ ประกอบมาตรา ๑๒ (๔) จัดให้มีระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อประโยชน์ในการอำนวยความสะดวกในการบริการประชาชน

ดังนั้นเพื่อให้หน่วยงานของรัฐสามารถดำเนินการเกี่ยวกับดิจิทัลไอดีตามที่ได้กล่าวข้างต้น จึงกำหนดแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม

๒. ขอบข่าย

แนวทางฯ ฉบับนี้ เป็นแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม สำหรับบุคคลธรรมดาและนิติบุคคล ที่ครอบคลุมถึงบทนิยาม กฎหมายและแนวปฏิบัติที่เกี่ยวข้องกับแบบจำลองดิจิทัลไอดี ภาพรวมของการพิสูจน์และยืนยันตัวตนทางดิจิทัล กลุ่มการให้บริการภาครัฐ การบริหารจัดการความเสี่ยง รวมถึงการทำความรู้จักผู้ใช้บริการ เพื่อให้หน่วยงานที่เกี่ยวข้องกับการใช้ดิจิทัลไอดีมีความเข้าใจตรงกัน โดยอ้างอิงข้อกำหนด ดังนี้

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

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

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

๒.๔ ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ [๔]

๒.๕ ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน [๕]

๒.๖ ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน [๖]

อย่างไรก็ตาม แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล ว่าด้วย การใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม ฉบับนี้ จะเป็นคำแนะนำโดยทั่วไปซึ่งไม่สามารถครอบคลุมประเด็นทางกฎหมายทั้งหมดที่อาจเกิดขึ้นได้ ดังนั้นหากมีข้อสงสัยเกี่ยวกับการดำเนินการตามเอกสารฉบับนี้หรือประเด็นอื่น ๆ ไม่ได้กล่าวถึงในที่นี้ ควรมีการปรึกษากับผู้เชี่ยวชาญทางกฎหมายตามความจำเป็น

๓. บทนิยาม

ความหมายของนิยามที่ใช้ในแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัลฯ ฉบับนี้มีดังนี้

๓.๑ บริการภาครัฐ หมายความว่า การดำเนินการอย่างหนึ่งอย่างใดที่หน่วยงานของรัฐจัดทำหรือจัดให้มีขึ้นหรือที่มอบอำนาจให้เอกชนดำเนินการแทนเพื่ออำนวยความสะดวกหรือตอบสนองความต้องการของประชาชน

๓.๒ คุณลักษณะ (Attribute) หมายความว่า ลักษณะ หรือคุณสมบัติของบุคคล [๔]

๓.๓ ไอเดนทิตี (Identity หรือ ID) หมายความว่า คุณลักษณะ หรือชุดของคุณลักษณะที่ใช้ระบุตัวบุคคลในบริบทที่กำหนด [๔]

๓.๔ ดิจิทัลไอดี (Digital Identity หรือ Digital ID) หมายความว่า คุณลักษณะ หรือชุดของคุณลักษณะที่ถูกรวบรวมและบันทึกในรูปแบบดิจิทัล ซึ่งสามารถใช้ระบุตัวบุคคลในบริบทที่กำหนด และสามารถใช้ทำธุรกรรมอิเล็กทรอนิกส์ [๔]

๓.๕ การลงทะเบียน (Enrolment) หมายความว่า กระบวนการที่ผู้สมัครใช้บริการลงทะเบียนเป็นผู้ใช้บริการของผู้พิสูจน์และยืนยันตัวตน [๔]

๓.๖ การพิสูจน์ตัวตน (Identity Proofing) หมายความว่า กระบวนการที่ผู้พิสูจน์และยืนยันตัวตนรวบรวมข้อมูลตรวจสอบหลักฐานแสดงตน และตรวจสอบตัวตนของผู้สมัครใช้บริการ [๔]

๓.๗ การยืนยันตัวตน (Authentication) หมายความว่า กระบวนการที่ผู้ใช้บริการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตนว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างด้วยการใช้สิ่งที่ใช้ยืนยันตัวตน [๔]

๓.๘ ผู้ให้บริการภาครัฐ หมายความว่า หน่วยงานของรัฐที่ให้บริการหรืออนุญาตให้เข้าถึงข้อมูลหรือระบบบริการภาครัฐ โดยอาศัยสิ่งที่ใช้ยืนยันตัวตนและผลการยืนยันตัวตนหรือสิ่งที่ใช้รับรองตัวตนจากผู้พิสูจน์และยืนยันตัวตน

๓.๙ ผู้พิสูจน์และยืนยันตัวตน (Identity Provider: IdP) หมายความว่า บุคคลหรือหน่วยงานที่น่าเชื่อถือซึ่งทำหน้าที่

(๑) รับลงทะเบียนและพิสูจน์ตัวตน และ

(๒) บริหารจัดการสิ่งที่ใช้รับรองตัวตน ซึ่งเชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ

โดยผู้พิสูจน์และยืนยันตัวตนอาจบริหารจัดการสิ่งที่ใช้รับรองตัวตนเพื่อใช้ภายในองค์กรหรือใช้ภายนอกองค์กรก็ได้ [๔]

๓.๑๐ แหล่งให้ข้อมูลที่น่าเชื่อถือ (Authoritative Source: AS) หมายความว่า หน่วยงานที่มีความน่าเชื่อถือและสามารถเข้าถึงหรือมีข้อมูลที่ถูกต้อง ซึ่งทำหน้าที่

(๑) ตรวจสอบข้อมูลหรือสถานะของหลักฐานแสดงตนของผู้ใช้บริการตามการร้องขอจากผู้พิสูจน์และยืนยันตัวตน หรือ

(๒) อนุญาตให้ผู้ให้บริการภาครัฐเข้าถึงข้อมูลที่น่าเชื่อถือหรือข้อมูลส่วนบุคคลซึ่งได้รับความยินยอมจากผู้ใช้บริการ

๓.๑๑ แหล่งออกหลักฐานแสดงตน (Issuing Source) หมายความว่า หน่วยงานที่รับผิดชอบในการจัดทำข้อมูล หลักฐานทางดิจิทัลหรือเอกสารที่ใช้เป็นหลักฐานแสดงตน

๓.๑๒ ผู้สมัครใช้บริการ (Applicant) หมายความว่า บุคคลที่สมัครใช้บริการพิสูจน์และยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน [๔]

๓.๑๓ ผู้ใช้บริการ (Subscriber) หมายความว่า ผู้สมัครใช้บริการที่ผ่านการลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตน และได้รับสิ่งที่ใช้ยืนยันตัวตนสำหรับใช้ยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน [๔]

๓.๑๔ สิ่งที่ใช้ยืนยันตัวตน (Authenticator) หมายความว่า สิ่งที่ผู้ใช้บริการครอบครองเพื่อใช้ในการยืนยันตัวตนโดยสิ่งที่ใช้ยืนยันตัวตนจะมีปัจจัยของการยืนยันตัวตนอย่างน้อยหนึ่งปัจจัย [๔]

๓.๑๕ สิ่งที่ใช้รับรองตัวตน (Credential) หมายความว่า เอกสาร วัตถุ หรือกลุ่มข้อมูล ที่เชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตน [๔]

๓.๑๖ เจ้าพนักงาน หมายความว่า บุคคลซึ่งกฎหมายบัญญัติว่าเป็นเจ้าพนักงานหรือได้รับแต่งตั้งตามกฎหมายให้ปฏิบัติหน้าที่ราชการ ไม่ว่าเป็นประจำหรือครั้งคราว และไม่ว่าจะได้รับค่าตอบแทนหรือไม่ [๘]

๔. กฎหมายและแนวปฏิบัติที่เกี่ยวข้อง

การใช้ดิจิทัลไอดีสำหรับบริการภาครัฐมีการบัญญัติไว้ในกฎหมาย หรือแนวปฏิบัติที่เกี่ยวข้อง ดังนี้

๔.๑ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ ในมาตรา ๑๒ (๔) กำหนดให้หน่วยงานของรัฐจัดให้มีระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อประโยชน์ในการอำนวยความสะดวกในการบริการประชาชน ซึ่งมีมาตรฐานและแนวทางที่สอดคล้องกันตามที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด

๔.๒ ประกาศสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (องค์การมหาชน) เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย ดังนี้

๔.๒.๑ ภาพรวมและอภิธานศัพท์ (ขมธอ. 18-2561) เป็นการอธิบายภาพรวมและอภิธานศัพท์เกี่ยวกับการใช้งานดิจิทัลไอดีสำหรับประเทศไทย การบริหารความเสี่ยง และการกำหนดระดับความน่าเชื่อถือ

๔.๒.๒ การลงทะเบียนและพิสูจน์ตัวตน (ขมธอ. 19-2561) เป็นการอธิบายข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน ในการลงทะเบียนและพิสูจน์ตัวตนของผู้สมัครใช้บริการที่ประสงค์จะทำธุรกรรมออนไลน์ด้วยดิจิทัลไอดี ตามระดับความน่าเชื่อถือของไอเดนทิตี

๔.๒.๓ การยืนยันตัวตน (ขมธอ. 20-2561) เป็นการอธิบายข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน ในการยืนยันตัวตนของผู้ใช้บริการที่ประสงค์จะทำธุรกรรมออนไลน์ด้วยดิจิทัลไอดี ตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

๕. แบบจำลองดิจิทัลไอดี (Digital Identity Model)

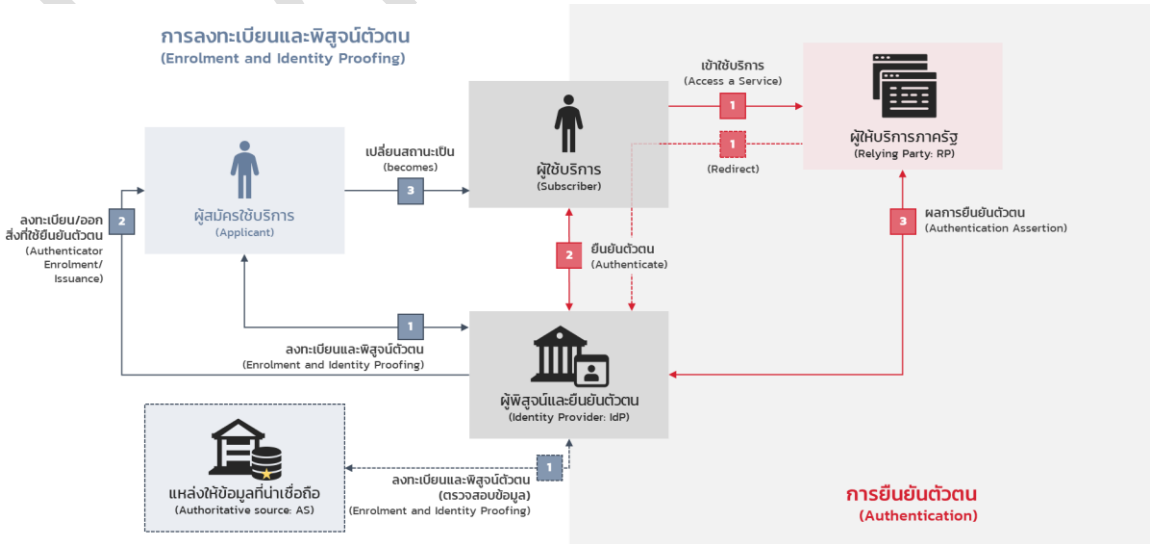
๕.๑ ภาพรวม (Overview)

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 (รายละเอียดจะกล่าวต่อไปในแนวทางฯ เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล)

เมื่อผู้ใช้บริการเข้าใช้บริการของผู้ให้บริการภาครัฐ (Relying Party: RP) จะต้องยืนยันตัวตนว่าเป็นบุคคลนั้นจริง หรือเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างนั้นจริง โดยแสดงให้ผู้พิสูจน์และยืนยันตัวตน (Identity Provider: IdP) เห็นว่าตนครอบครองสิ่งที่ใช้ยืนยันตัวตนตามเกณฑ์ที่กำหนด เมื่อผู้พิสูจน์และยืนยันตัวตนตรวจสอบความถูกต้องจะส่งผลการยืนยันตัวตนให้กับผู้ให้บริการ โดยผู้ให้บริการสามารถใช้ข้อมูลที่อยู่ในผลการยืนยันตัวตนไปพิจารณาสิทธิ ทั้งนี้ต้องมีกระบวนการที่ผู้ใช้บริการอนุญาตให้ผู้ให้บริการเข้าถึงข้อมูลของตน (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 ซึ่งมีขั้นตอนดังนี้

(๑) ผู้สมัครใช้บริการลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตน โดยผู้พิสูจน์และยืนยันตัวตนอาจตรวจสอบข้อมูลกับผู้ให้ข้อมูลที่น่าเชื่อถือ

(๒) หากพิสูจน์ตัวตนสำเร็จ ผู้พิสูจน์และยืนยันตัวตนจะลงทะเบียนหรือออกสิ่งที่ใช้ยืนยันตัวตน และสร้างสิ่งที่ใช้รับรองตัวตนให้กับผู้ใช้บริการ

(๓) ผู้สมัครใช้บริการ เปลี่ยนสถานะเป็น ผู้ใช้บริการ

หมายเหตุ ผู้พิสูจน์และยืนยันตัวตน ต้องเก็บรักษาสิ่งที่ใช้รับรองตัวตน สถานะของสิ่งที่ใช้รับรองตัวตน และข้อมูลที่ใช้ในกระบวนการลงทะเบียน ตลอดอายุการใช้งานของสิ่งที่ใช้รับรองตัวตน (เป็นอย่างน้อย) ส่วนผู้ใช้บริการต้องเก็บรักษาสิ่งที่ใช้ยืนยันตัวตน

จากรูปที่ ๑ ด้านขวา เป็นกระบวนการยืนยันตัวตน ซึ่งมีขั้นตอนดังนี้

(๑) ผู้ใช้บริการ ขอเข้าใช้บริการกับผู้ให้บริการ โดยผู้ให้บริการภาครัฐอาจให้ผู้ใช้บริการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน (Redirect)

(๒) ผู้พิสูจน์และยืนยันตัวตน ต้องตรวจสอบสิ่งที่ใช้ยืนยันตัวตนที่เชื่อมโยงไอเดนทิตีของผู้ใช้บริการ

๕.๒ การลงทะเบียนและพิสูจน์ตัวตน (Enrolment and Identity Proofing)

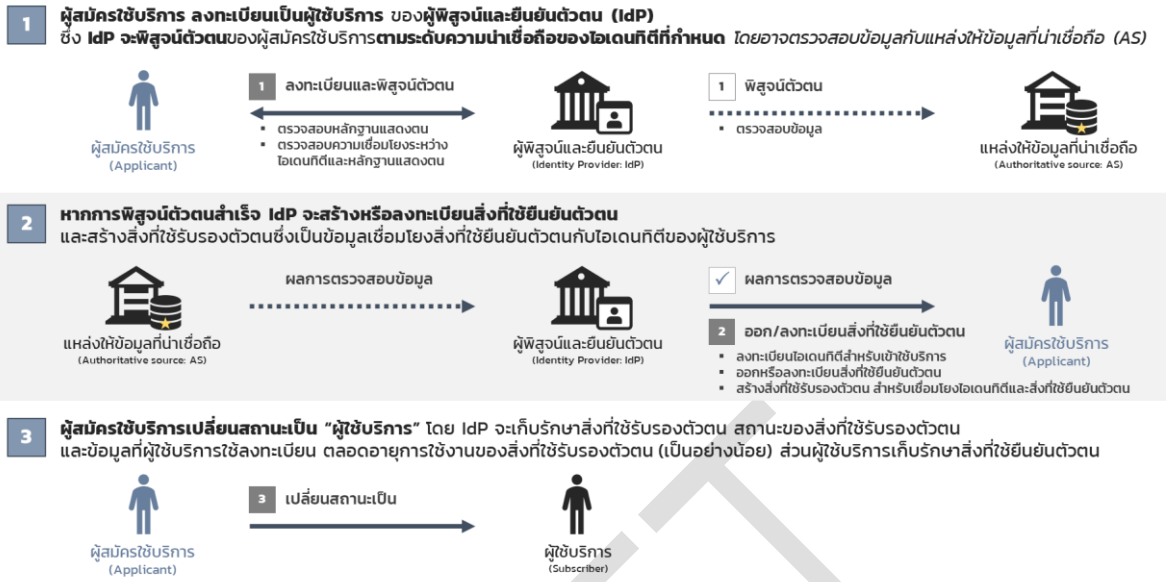
๕.๒.๑ การลงทะเบียน (Enrolment)

เป็นกระบวนการได้มาและการบันทึกข้อมูลไอเดนทิตีที่จำเป็นจากผู้สมัครใช้บริการ ซึ่งอ้างอิงมาจากข้อมูลประวัติ เช่น ชื่อ ชื่อสกุล วันเดือนปีเกิด เพศ ที่อยู่ อีเมล และได้จากข้อมูลชีวมิติ (Biometric) เช่น ลายนิ้วมือ รูม่านตา รวมถึงการนำคุณลักษณะอื่น ๆ เพิ่มเติมประกอบเข้าด้วยกัน สำหรับบัตรประจำตัวประชาชน จะต้องได้ข้อมูลอย่างน้อยเช่น เลขประจำตัวประชาชน ชื่อ ชื่อสกุล วันเดือนปีเกิด เลขหลังบัตรประจำตัวประชาชน (Laser Code) โดยคุณลักษณะดังกล่าวจะต้องแสดงให้เห็นว่าไอเดนทิตีที่ได้มามีความน่าเชื่อถือ มีเพียงหนึ่งเดียว และมีความเฉพาะเจาะจงภายในบริบทของผู้ใช้บริการทั้งหมดที่ผู้พิสูจน์และยืนยันตัวตนดูแล

๕.๒.๒ การพิสูจน์ตัวตน (Identity Proofing)

เป็นกระบวนการตรวจสอบหลักฐานแสดงตนและตรวจสอบตัวบุคคล เมื่อมีผู้สมัครใช้บริการอ้างความเป็นเจ้าของไอเดนทิตีในระหว่างการลงทะเบียนนั้น ทำให้ไอเดนทิตีถูกตรวจสอบโดยเปรียบเทียบกับคุณลักษณะของข้อมูลที่มีอยู่ ดังนั้นกระบวนการพิสูจน์ตัวตนดังกล่าว ทำให้มั่นใจได้ว่าไอเดนทิตีนั้นมีอยู่จริง เช่น การตรวจสอบเพื่อยืนยันว่าผู้สมัครใช้บริการเป็นบุคคลนั้นจริงและมีเพียงหนึ่งเดียว โดยอาจตรวจสอบไอเดนทิตีที่กล่าวอ้างกับไอเดนทิตีบนฐานข้อมูลแห่งอื่น เช่น ระบบทะเบียนราษฎร์ หลังจากนั้นผู้พิสูจน์และยืนยันตัวตนจะออกสิ่งที่ใช้รับรองตัวตนในรูปแบบดิจิทัลเพื่อใช้ในกระบวนการยืนยันตัวตน เช่น บัตรประจำตัวประชาชน หนังสือเดินทาง ใบรับรองอิเล็กทรอนิกส์

๕.๒.๓ กระบวนการลงทะเบียนและพิสูจน์ตัวตน (Enrolment and Identity Proofing Process)



รูปที่ ๒ กระบวนการลงทะเบียนและพิสูจน์ตัวตน

ที่มา: ปรับปรุงจาก (ขมธอ. 18-2561 ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์) [๔]

จากรูปที่ ๒ ประกอบด้วย ๓ กระบวนการ ดังนี้

(๑) ผู้สมัครใช้บริการลงทะเบียนกับผู้พิสูจน์และยืนยันตัวตนที่ตนต้องการใช้บริการพิสูจน์และยืนยันตัวตน ซึ่งผู้พิสูจน์และยืนยันตัวตนจะดำเนินการพิสูจน์ตัวตนของผู้สมัครใช้บริการ โดยรวบรวมข้อมูลเพื่อระบุตัวตน ตรวจสอบหลักฐานแสดงตน และตรวจสอบตัวบุคคลตามระดับความน่าเชื่อถือของไอเดนทิตีที่กำหนด ทั้งนี้อาจตรวจสอบข้อมูลกับแหล่งให้ข้อมูลที่น่าเชื่อถือ

(๒) หากการพิสูจน์ตัวตนสำเร็จ ผู้พิสูจน์และยืนยันตัวตนจะดำเนินการดังนี้

(ก) ลงทะเบียนไอเดนทิตีที่ใช้ระบุตัวตนผู้ใช้บริการแต่ละราย เช่น สร้างเลขประจำตัวให้กับผู้ใช้บริการหรือลงทะเบียนชื่อผู้ใช้บริการ (User ID) ที่ไม่ซ้ำกัน

(ข) ออกหรือลงทะเบียนสิ่งที่ใช้ยืนยันตัวตนให้กับผู้ใช้บริการ โดยชนิดของสิ่งที่ใช้ยืนยันตัวตนขึ้นอยู่กับระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

(ค) สร้างสิ่งที่ใช้รับรองตัวตนซึ่งเป็นข้อมูลเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตีของผู้ใช้บริการ เพื่อให้ผู้ใช้บริการสามารถนำสิ่งที่ใช้ยืนยันตัวตนดังกล่าวมาใช้ยืนยันตัวตนในอนาคต

(๓) ผู้สมัครใช้บริการเปลี่ยนสถานะเป็น “ผู้ใช้บริการ” โดยผู้พิสูจน์และยืนยันตัวตนจะเก็บรักษาสิ่งที่ใช้รับรองตัวตน สถานะของสิ่งที่ใช้รับรองตัวตน และข้อมูลที่ผู้ใช้บริการใช้ลงทะเบียน ตลอดอายุการใช้งานของสิ่งที่ใช้รับรองตัวตน (เป็นอย่างน้อย) ส่วนผู้ใช้บริการเก็บรักษาสิ่งที่ใช้ยืนยันตัวตน

๕.๓ การยืนยันตัวตน (Authentication)

๕.๓.๑ สิ่งที่ใช้ยืนยันตัวตน (Authenticators)

สิ่งที่ใช้ยืนยันตัวตน คือ สิ่งที่ผู้ใช้บริการครอบครองและใช้ในการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตนว่าเป็นบุคคลที่กล่าวอ้างจริง สิ่งที่ใช้ยืนยันตัวตนอาจประกอบด้วยปัจจัยของการยืนยันตัวตนเพียงหนึ่งปัจจัยหรือมากกว่าหนึ่งปัจจัยก็ได้ อย่างไรก็ตาม ความปลอดภัยของระบบยืนยันตัวตน (Authentication System) ขึ้นอยู่กับความสามารถในการป้องกันการโจมตีของสิ่งที่ใช้ยืนยันตัวตนและจำนวนปัจจัยของการยืนยันตัวตน โดยปัจจัยของการยืนยันตัวตน (Authentication Factor) แบ่งออกเป็น ๓ ประเภท ดังนี้

- สิ่งที่ผู้ใช้บริการรู้ (Something You Know) คือ ข้อมูลที่ผู้ใช้บริการเท่านั้นที่ทราบ เช่น รหัสผ่าน
- สิ่งที่ผู้ใช้บริการมี (Something You Have) คือ สิ่งที่ผู้ใช้บริการเท่านั้นที่ครอบครอง เช่น บัตรประจำตัวประชาชน
- สิ่งที่ผู้ใช้บริการเป็น (Something You Are) คือ ข้อมูลทางชีวมิติของผู้ใช้บริการเท่านั้น เช่น ลายนิ้วมือ ใบหน้า

ข้อมูลลับ (Secrets) ที่อยู่ในสิ่งที่ใช้ยืนยันตัวตนเป็นได้ทั้งกุญแจแบบอสมมาตร (การเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสคนละตัว คือกุญแจสาธารณะและกุญแจส่วนตัว) หรือกุญแจแบบสมมาตร (การเข้ารหัสและถอดรหัสโดยใช้กุญแจรหัสตัวเดียวกัน) ในกรณีกุญแจแบบอสมมาตร ผู้ใช้บริการจะใช้กุญแจส่วนตัว (Private Key) ที่อยู่ในสิ่งที่ใช้ยืนยันตัวตนเพื่อยืนยันตัวตน โดยผู้พิสูจน์และยืนยันตัวตนจะใช้กุญแจสาธารณะ (Public Key) กับกุญแจส่วนตัว (Private Key) ของผู้ที่กล่าวอ้างมาจับคู่กัน (Key Pairs) เพื่อพิสูจน์ความเป็นเจ้าของและครอบครองสิ่งที่ใช้ยืนยันตัวตนนั้นจริง อนึ่ง ข้อมูลลับที่ใช้รหัสตัวเดียวกัน (Shared Secret) ที่อยู่ในสิ่งที่ใช้ยืนยันตัวตนอาจเป็นได้ทั้งกุญแจแบบสมมาตร หรือรหัสลับจดจำ (Memorized Secret) โดยข้อแตกต่างระหว่างกุญแจแบบสมมาตรและรหัสลับจดจำ คือ กุญแจแบบสมมาตรมักสร้างจากระบบสุ่มและเก็บไว้ในอุปกรณ์ฮาร์ดแวร์หรือซอฟต์แวร์ ในขณะที่รหัสลับจดจำเป็นข้อมูลที่ผู้ใช้บริการสามารถจดจำได้

การยืนยันตัวตนแบบหลายปัจจัย (Multi-factor Authentication) สามารถทำได้ ๒ รูปแบบ ดังนี้

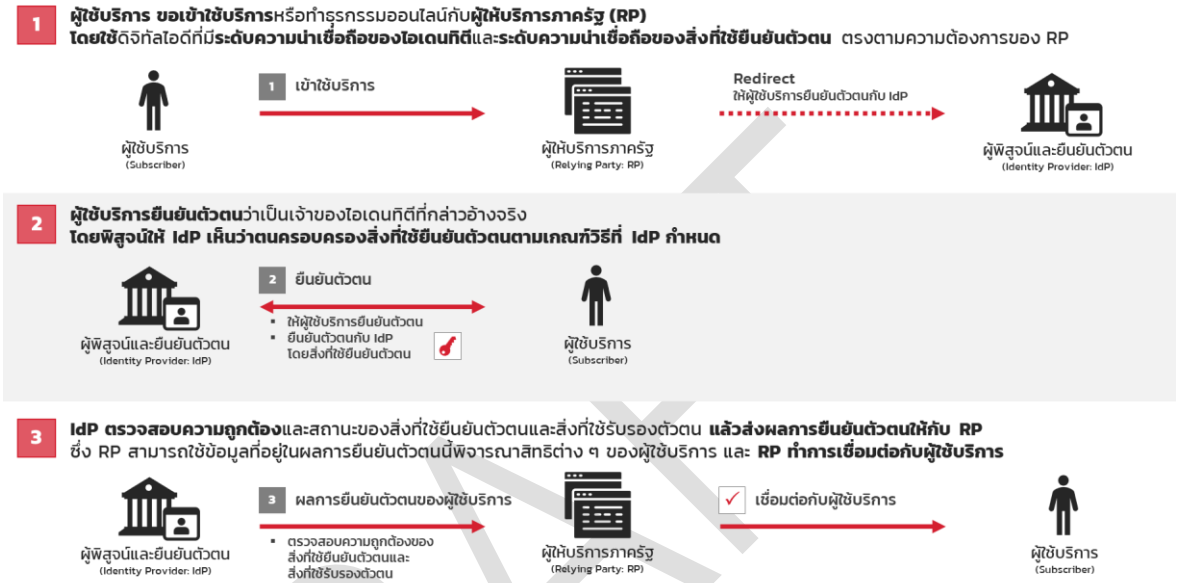
- ใช้การยืนยันตัวตนมากกว่าหนึ่งปัจจัย เช่น ผู้ใช้บริการต้องใช้รหัสผ่าน (สิ่งที่ผู้ใช้บริการรู้) และรหัสผ่านแบบใช้ครั้งเดียวที่ได้รับทางโทรศัพท์เคลื่อนที่ (สิ่งที่ผู้ใช้บริการมี) เพื่อยืนยันตัวตน
- มีอย่างน้อยหนึ่งปัจจัยที่ปกป้องข้อมูลลับ เช่น ใช้อุปกรณ์ฮาร์ดแวร์ที่มีวิธีการเข้ารหัสลับ (สิ่งที่ผู้ใช้บริการมี) และใช้ลายนิ้วมือ (สิ่งที่ผู้ใช้บริการเป็น) ในการเข้าถึงอุปกรณ์ดังกล่าวนั้น เพื่อยืนยันตัวตน

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

๕.๓.๒ สิ่งที่ใช้รับรองตัวตน (Credentials)

สิ่งที่ใช้รับรองตัวตน คือ การเชื่อมโยงไอเดนทิตีของผู้ใช้บริการเข้ากับสิ่งที่ใช้ยืนยันตัวตน ซึ่งสิ่งที่ใช้รับรองตัวตนจะถูกเก็บและดูแลโดยผู้พิสูจน์และยืนยันตัวตน เช่น ฐานข้อมูลที่เชื่อมโยงไอเดนทิตีของผู้ใช้บริการเข้ากับสิ่งที่ใช้ยืนยันตัวตน ในขณะที่ผู้ใช้บริการจะครอบครองสิ่งที่ใช้ยืนยันตัวตน เช่น กุญแจส่วนตัว PIN รหัสผ่าน แต่ไม่จำเป็นต้องครอบครองสิ่งที่ใช้รับรองตัวตน

๕.๓.๓ กระบวนการยืนยันตัวตน (Authentication Process)



รูปที่ ๓ กระบวนการยืนยันตัวตน

ที่มา: ปรับปรุงจาก (ขมธอ. 18-2561 ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์) [๔]

จากรูปที่ ๓ เมื่อผู้สมัครใช้บริการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลสำเร็จ และถูกปรับสถานะเป็นผู้ใช้บริการเรียบร้อยแล้ว ในกรณีที่ต้องการเข้าใช้บริการภาครัฐของผู้ให้บริการภาครัฐจะมีกระบวนการ ๓ กระบวนการ ดังนี้

(๑) ผู้ใช้บริการขอเข้าใช้บริการ และผู้ให้บริการภาครัฐต้องการทราบว่าผู้ใช้บริการเป็นผู้ใด สำหรับผู้ใช้บริการเคยลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตนที่ผู้ให้บริการภาครัฐเชื่อถือ ผู้ให้บริการภาครัฐจะนำผู้ใช้บริการ (Redirect) ไปยังหน้าต่างยืนยันตัวตนของผู้พิสูจน์และยืนยันตัวตนนั้น

(๒) ผู้ใช้บริการต้องยืนยันตัวตนด้วยการแสดงสิ่งที่ใช้ยืนยันตัวตนต่อผู้พิสูจน์และยืนยันตัวตนโดยพิสูจน์ให้เห็นว่าตนครอบครองสิ่งที่ใช้ยืนยันตัวตนตามเกณฑ์วิธีที่ผู้พิสูจน์และยืนยันตัวตนกำหนด

(๓) เมื่อผู้พิสูจน์และยืนยันตัวตนตรวจสอบสิ่งที่ใช้ยืนยันตัวตนและสิ่งที่ใช้รับรองตัวตนเรียบร้อยแล้ว ผู้พิสูจน์และยืนยันตัวตนจะส่งผลการยืนยันตัวตนให้กับผู้ให้บริการภาครัฐ เพื่อให้ผู้ให้บริการภาครัฐนำไปใช้พิจารณาอนุญาตเข้าใช้บริการภาครัฐ หรือให้เข้าถึงข้อมูลหรือระบบต่อไป

๖. การจำแนกกลุ่มการให้บริการภาครัฐในรูปแบบดิจิทัล (Government Digital Service Classification)

เนื่องด้วยการให้บริการภาครัฐมีรูปแบบที่หลากหลาย เพื่อให้เกิดความชัดเจนในการให้บริการ จึงจำแนกกลุ่มการให้บริการภาครัฐในรูปแบบดิจิทัลออกเป็น ๔ กลุ่ม [๙] ดังนี้

๖.๑ กลุ่มการให้บริการข้อมูลพื้นฐาน (Emerging Services)

เป็นการให้บริการเผยแพร่ข้อมูลข่าวสารทั่วไปของหน่วยงานของรัฐ เช่น นโยบายสาธารณะ การกำกับดูแล กฎหมาย ระเบียบ เอกสารที่เกี่ยวข้อง และประเภทการให้บริการภาครัฐ ผ่านทางเว็บไซต์หรือช่องทางให้บริการข่าวสารข้อมูลอื่น โดยมีแนวทางการพิจารณากลุ่มการให้บริการข้อมูลพื้นฐาน อย่างน้อยดังนี้

- เป็นข้อมูลเปิดสาธารณะหรือข้อมูลทั่วไป
- ไม่จำเป็นต้องใช้ข้อมูลส่วนบุคคล
- ไม่จำเป็นต้องมีการลงทะเบียนและพิสูจน์ตัวตน

๖.๒ กลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ (Enhanced Services)

เป็นการให้บริการข้อมูลข่าวสารของหน่วยงานของรัฐในรูปแบบการสื่อสารทางเดียวหรือสองทางกับผู้ใช้บริการ เช่น การรับแจ้งเรื่องร้องเรียน ข้อเสนอแนะ หรือแสดงความคิดเห็น ผ่านทางเว็บไซต์หรือช่องทางให้บริการข่าวสารข้อมูลอื่น โดยมีแนวทางการพิจารณากลุ่มการให้บริการข้อมูลที่มีการปฏิสัมพันธ์กับผู้ใช้บริการ อย่างน้อยดังนี้

- มีการสื่อสารโต้ตอบกับผู้ใช้บริการ
- ใช้ข้อมูลส่วนบุคคลหรือไม่ก็ได้ โดยเจ้าของข้อมูลส่วนบุคคลไม่จำเป็นต้องเป็นผู้ดำเนินการเอง
- มีการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลหรือไม่ก็ได้
- มีช่องทางที่สามารถติดต่อได้

๖.๓ กลุ่มการให้บริการธุรกรรม (Transactional Services)

เป็นการให้บริการธุรกรรมของหน่วยงานของรัฐซึ่งมีผลผูกพันทางกฎหมาย เช่น การอนุญาต การจดทะเบียน หรือการดำเนินการใด ๆ กับหน่วยงานของรัฐ โดยมีแนวทางการพิจารณากลุ่มการให้บริการธุรกรรม อย่างน้อยดังนี้

- ต้องใช้ข้อมูลส่วนบุคคล เช่น เลขประจำตัวประชาชน ๑๓ หลัก โดยเจ้าของข้อมูลส่วนบุคคลต้องเป็นผู้ดำเนินการเอง ณ ขณะนั้น
- ต้องมีการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัล
- ต้องยืนยันช่องทางการติดต่อ เช่น หมายเลขโทรศัพท์ หรือ อีเมล

๖.๔ กลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงาน (Connected Services)

เป็นการให้บริการธุรกรรมที่มีการเชื่อมโยงข้อมูลระหว่างหน่วยงานเข้าด้วยกัน และมีผลผูกพันทางกฎหมาย เช่น การขอรับบริการภาครัฐแบบเบ็ดเสร็จ ณ จุดเดียว โดยมีแนวทางการพิจารณากลุ่มการให้บริการธุรกรรมที่เชื่อมโยงข้อมูลระหว่างหน่วยงาน อย่างน้อยดังนี้

- ต้องมีการเชื่อมโยงหรือใช้ข้อมูลร่วมกับหน่วยงานภายนอกแห่งอื่น
- ต้องใช้ข้อมูลส่วนบุคคล เช่น เลขประจำตัวประชาชน ๑๓ หลัก โดยเจ้าของข้อมูลส่วนบุคคลต้องเป็นผู้ดำเนินการเอง ณ ขณะนั้น หรือมีการมอบอำนาจ
- ในการลงทะเบียนและพิสูจน์ตัวตนครั้งแรก ต้องมีการพบเห็นต่อหน้า หรือ เสมือนพบเห็นต่อหน้า โดยต้องดำเนินการต่อหน้าเจ้าพนักงานที่มีอำนาจหน้าที่รับผิดชอบและผ่านการอบรม
- ต้องยืนยันช่องทางการติดต่อ เช่น หมายเลขโทรศัพท์ หรือ อีเมล

๗. การบริหารความเสี่ยงของดิจิทัลไอดี (Digital Identity Risk Management)

๗.๑ ภาพรวม (Overview)

ความเสี่ยงของการใช้ดิจิทัลไอดีตามแนวทางฯ ฉบับนี้ แบ่งออกเป็น ๒ ด้าน ดังนี้

(๑) การพิสูจน์ตัวตนผิดพลาด เช่น ผู้สมัครใช้บริการแอบอ้างไอเดนทิตีของบุคคลอื่นในการลงทะเบียน

(๒) การยืนยันตัวตนผิดพลาด เช่น ผู้ที่กล่าวอ้างใช้สิ่งที่ใช้ยืนยันตัวตนที่ไม่ใช่ของตนในการเข้าใช้บริการภาครัฐ

การประเมินความเสี่ยงในกระบวนการพิสูจน์และยืนยันตัวตน เพื่อช่วยให้สามารถเลือกใช้เทคโนโลยีหรือกลยุทธ์ที่เหมาะสมในการบรรเทาความเสี่ยงที่อาจเกิดขึ้น โดยวิธีการสำคัญในการประเมินความเสี่ยงดังกล่าว คือ การใช้วิธีการพิสูจน์ตัวตนและวิธีการยืนยันตัวตนที่มีความเข้มงวดสอดคล้องกับระดับผลกระทบและโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น

๗.๒ ระดับความน่าเชื่อถือ (Assurance Levels)

ผู้ให้บริการภาครัฐต้องกำหนดระดับความน่าเชื่อถือของแต่ละบริการตามผลการประเมินความเสี่ยง ซึ่งแบ่งระดับความน่าเชื่อถือออกเป็น ๒ ด้าน ดังนี้

๗.๒.๑ 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 รวมถึงตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างการพิสูจน์ตัวตนที่ระดับ IAL2 สามารถทำได้ทั้งแบบพบเห็นต่อหน้า หรือ แบบไม่พบเห็นต่อหน้า

ทั้งนี้ ผู้พิสูจน์และยืนยันตัวตน ที่รองรับระดับ IAL2 สามารถส่งผลการยืนยันตัวตนให้กับผู้ให้บริการภาครัฐที่ให้บริการที่ต้องการระดับ IAL1 ได้ หากผู้ใช้บริการให้ความยินยอม เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงปานกลางถึงความเสี่ยงสูง

(๓) ระดับความน่าเชื่อถือของไอเดนทิตี ระดับที่ ๓ (IAL3)

เพิ่มความเข้มงวดให้กับข้อกำหนดที่ระดับ IAL2 ด้วยการพิจารณาหลักฐานแสดงตนเพิ่มเติมและการตรวจสอบข้อมูลชีวมิติ เพื่อป้องกันการปลอมตัวเป็นบุคคลอื่น การหลอกลวงการลงทะเบียนซ้ำ หรือความเสียหายอื่น ๆ การพิสูจน์ตัวตนที่ระดับ IAL3 สามารถทำได้เฉพาะแบบพบเห็นต่อหน้า ซึ่งรวมถึงแบบเสมือนพบเห็นต่อหน้า

ทั้งนี้ ผู้พิสูจน์และยืนยันตัวตน ที่รองรับระดับ IAL3 สามารถส่งผลการยืนยันตัวตนให้กับผู้ให้บริการภาครัฐที่ให้บริการที่ต้องการระดับ IAL1 และ IAL2 ได้ หากผู้ใช้บริการให้ความยินยอม เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงสูง

๗.๒.๒ 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 ปัจจัยขึ้นไปที่แตกต่างกัน เพื่อเพิ่มความน่าเชื่อถือในการยืนยันตัวตนแต่ละครั้ง เช่น ผู้ใช้บริการแสดงรหัสผ่านเข้าระบบ ซึ่งรหัสผ่านเป็นสิ่งที่ผู้ใช้บริการรู้ และแสดงรหัสผ่านแบบใช้ครั้งเดียวที่ได้รับผ่านทางหมายเลขโทรศัพท์ ซึ่งเป็นสิ่งที่ผู้ใช้บริการมี

จำนวนและประเภทของปัจจัยของการยืนยันตัวตนมีผลกับระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน โดยระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน คือ ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของผู้ใช้บริการ ซึ่งการกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนที่เหมาะสมจะช่วยลดโอกาสของการยืนยันตัวตนผิดพลาด แบ่งออกเป็น ๓ ระดับ ดังนี้

(๑) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ระดับที่ ๑ (AAL1)

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

(๒) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ระดับที่ ๒ (AAL2)

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

ระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตนต้องเป็นโพรโทคอลที่มีความปลอดภัย เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงปานกลางถึงความเสี่ยงสูง

(๓) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ระดับที่ ๓ (AAL3)

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

๗.๒.๓ ข้อกำหนดของการเลือกระดับความน่าเชื่อถือของไอเดนทิตีและระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

ในการเลือกระดับความน่าเชื่อถือสามารถทำแยกจากกันได้เพื่อให้เกิดความยืดหยุ่นในการให้บริการของหน่วยงานของรัฐ อย่างไรก็ตาม มีข้อจำกัดเกี่ยวกับข้อมูลส่วนบุคคลของผู้ใช้บริการที่ใช้ลงทะเบียนกับผู้พิสูจน์และยืนยันตัวตน และสิ่งที่ใช้ยืนยันตัวตนที่จะป้องกันการเข้าถึงข้อมูลดังกล่าวจากบุคคลที่ไม่ได้รับอนุญาตต้องมีความสอดคล้องกัน ดังนั้นต้องมีการจัดกลุ่มการใช้ระดับความน่าเชื่อถือของไอเดนทิตีและระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนบางระดับ 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

๗.๓ ความเสี่ยงและผลกระทบ (Risk and Impacts)

การประเมินความเสี่ยง (Risk Assessment) เป็นการวิเคราะห์และประเมินระดับความเสี่ยงที่ส่งผลกระทบเมื่อมีการพิสูจน์หรือยืนยันตัวตนผิดพลาด โดยพิจารณาจากระดับผลกระทบ (Impact) และโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้น (Likelihood) [๑][๑๒] โดยผู้ให้บริการภาครัฐต้องพิจารณาถึงผลกระทบ ระดับความรุนแรง และโอกาสหรือความเป็นไปได้ที่อาจจะเกิดขึ้นได้หากการพิสูจน์หรือยืนยันตัวตนผิดพลาด ทั้งนี้ผลลัพธ์ที่ได้จะนำใช้ในการกำหนดระดับความน่าเชื่อถือของไอเดนทิตี และระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน โดยดำเนินการ ดังนี้

(๑) ระบุประเภทของผลกระทบ (Categories of Harm)

จากข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ [๔] แบ่งประเภทของผลกระทบเป็น ๖ ด้าน ดังนี้

- ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง
- ความเสียหายทางการเงิน
- ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ
- การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
- ความปลอดภัยของบุคคล
- การละเมิดทางแพ่งหรือทางอาญา

ทั้งนี้อาจเพิ่มเติมประเภทของผลกระทบอื่น ๆ ให้สอดคล้องกับนโยบายด้านความเสี่ยงของหน่วยงานของตนได้

(๒) วิเคราะห์ผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาดในแต่ละด้าน (Impact Levels)

การประเมินระดับผลกระทบที่เป็นไปได้ จะใช้วิธีการพิจารณาระดับผลกระทบที่สามารถเกิดขึ้นได้เมื่อเกิดข้อผิดพลาดในแต่ละด้าน ดังตารางที่ ๒

ตารางที่ ๒ เกณฑ์การพิจารณาระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด

ผลกระทบ	ระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด		
	ต่ำ	ปานกลาง	สูง
ความไม่สะดวกสบายและเสื่อมเสียชื่อเสียง	มีความไม่สะดวกสบายและเสื่อมเสียชื่อเสียงในระยะสั้น และจำกัด	มีความไม่สะดวกสบายและเสื่อมเสียชื่อเสียงรุนแรง ระยะสั้น หรือมีผลปานกลางในระยะยาว	มีความไม่สะดวกสบายและเสื่อมเสียชื่อเสียงระยะยาว หรือมีผลกระทบหลายบุคคล
ความเสียหายทางการเงิน	มีความเสียหายทางการเงินที่ไม่มีนัยสำคัญ	มีความเสียหายทางการเงินรุนแรง	มีความเสียหายทางการเงินรุนแรงมาก
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบที่จำกัดต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงมากต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้	มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้	มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้

ผลกระทบ	ระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด		
	ต่ำ	ปานกลาง	สูง
	รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับต่ำ	รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับปานกลาง	รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับสูง
ความปลอดภัยของบุคคล	บาดเจ็บเล็กน้อย ไม่ต้องรับการรักษาพยาบาล	มีความเสี่ยงพอสมควรที่จะบาดเจ็บเล็กน้อย หรือมีความเสี่ยงจำกัดที่จะบาดเจ็บซึ่งต้องการการรักษาพยาบาล	มีความเสี่ยงที่จะบาดเจ็บสาหัส หรือถึงแก่ชีวิต
การละเมิดทางแพ่งหรือทางอาญา	การฝ่าฝืนกฎหมายนั้นเป็นเรื่องเล็กน้อย ซึ่งไม่จำเป็นต้องมีการบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงที่จะถูกบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงสูงเป็นพิเศษในการที่จะถูกบังคับใช้กฎหมาย

(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

(๔) วัดผลความเสี่ยง (Risk Evaluation)

พิจารณาจากความสัมพันธ์ระหว่างผลกระทบและโอกาสหรือความเป็นไปได้ที่จะเกิดขึ้นว่ามีความเสี่ยงระดับใด ดังตารางที่ ๔

ตารางที่ ๔ เกณฑ์การวัดผลความเสี่ยง

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

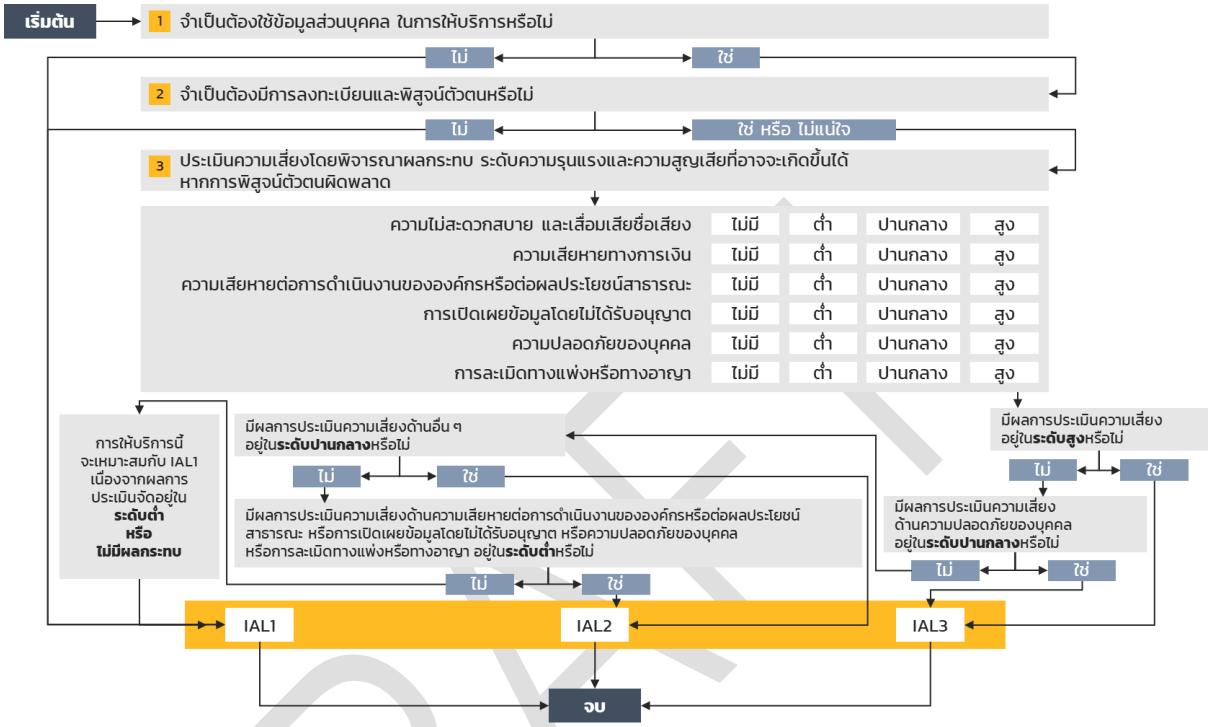
พิจารณาความหมายของแต่ละระดับความเสี่ยง ดังตารางที่ ๕

ตารางที่ ๕ ความหมายของแต่ละระดับความเสี่ยง

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

๘. การกำหนดระดับความน่าเชื่อถือของไอเดนทิตี (Selecting Identity Assurance Levels)

ผู้ให้บริการภาครัฐต้องกำหนดระดับความน่าเชื่อถือของไอเดนทิตี โดยนำผลของการประเมินความเสี่ยงมาประกอบกับการพิจารณาเพิ่มเติมที่เกี่ยวข้องกับการพิสูจน์ตัวตน 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

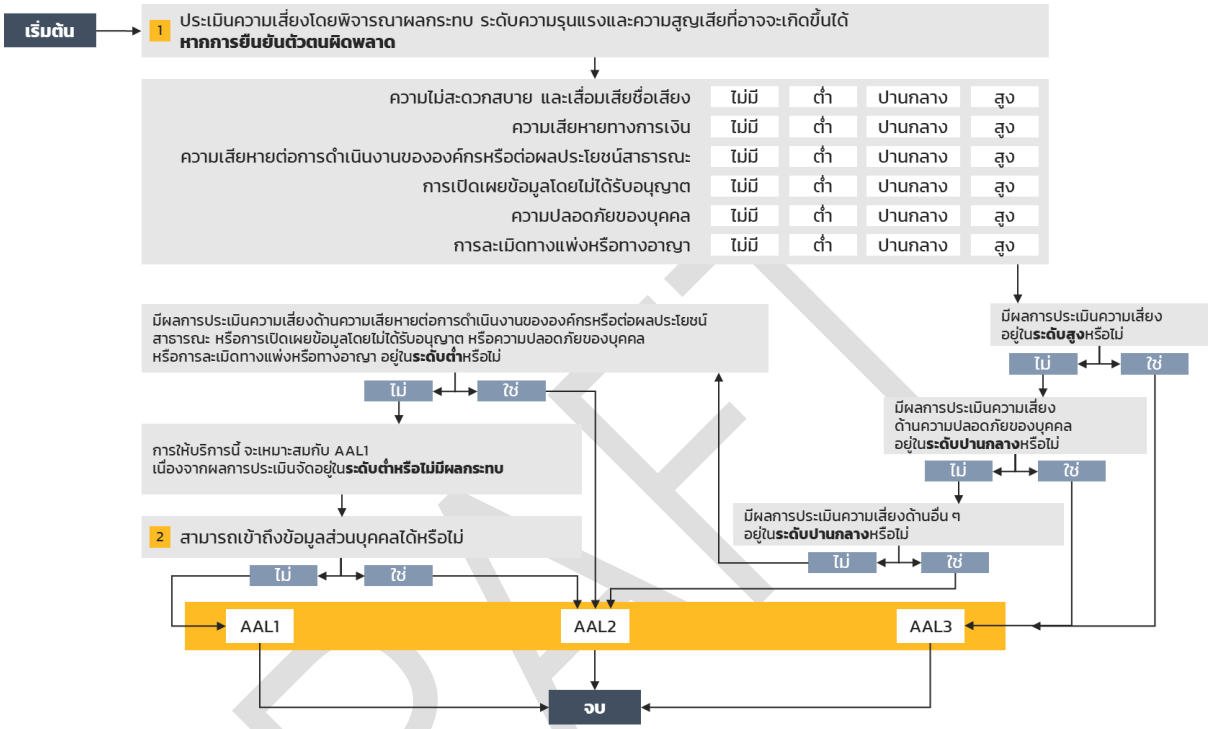
- กรณีที่ผลกระทบที่เป็นไปได้ด้านในด้านหนึ่งอยู่ในระดับสูง ให้กำหนดเป็น **ระดับ** IAL3
- กรณีที่ผลกระทบด้านความปลอดภัยของบุคคลอยู่ในระดับปานกลาง ให้กำหนดเป็น **ระดับ** IAL3
- กรณีที่ผลกระทบด้านอื่น ๆ อยู่ในระดับปานกลาง ให้กำหนดเป็น **ระดับ** IAL2
- กรณีที่ผลกระทบด้านความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต หรือความปลอดภัยของบุคคล หรือการละเมิดทางแพ่งหรือทางอาญาอยู่ในระดับต่ำ ให้กำหนดเป็น **ระดับ** IAL2
- กรณีที่นอกเหนือจากนี้ ให้กำหนดเป็น **ระดับ** IAL1

ตารางที่ ๖ การจัดระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือของไอเดนทิตีของผลกระทบในแต่ละด้าน

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

๙. 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

- กรณีที่ผลกระทบที่เป็นไปได้ด้านในด้านหนึ่งอยู่ในระดับสูง ให้กำหนดเป็น **ระดับ** AAL3
- กรณีที่ผลกระทบด้านความปลอดภัยของบุคคลอยู่ในระดับปานกลาง ให้กำหนดเป็น **ระดับ** AAL3
- กรณีที่ผลกระทบด้านอื่น ๆ อยู่ในระดับปานกลาง ให้กำหนดเป็น **ระดับ** AAL2
- กรณีที่ผลกระทบด้านความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต หรือความปลอดภัยของบุคคล หรือการละเมิดทางแพ่งหรือทางอาญาอยู่ในระดับต่ำ ให้กำหนดเป็น **ระดับ** AAL2
- กรณีที่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ ใช่หรือไม่ ถ้าใช่ ให้กำหนดเป็น **ระดับ** AAL2
- กรณีที่นอกเหนือจากนี้ ให้กำหนดเป็น **ระดับ** AAL1

ตารางที่ ๗ การจัดระดับความเสี่ยงเทียบกับระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนของผลกระทบในแต่ละด้าน

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

๑๐. การทำความรู้จักผู้ใช้บริการ (Know Your Customer)

การทำความรู้จักผู้ใช้บริการ อ้างอิงจากประกาศธนาคารแห่งประเทศไทย ที่ สนส. ๑๙/๒๕๖๒ เรื่อง หลักเกณฑ์การรู้จักลูกค้า (Know Your Customer: KYC) สำหรับการเปิดบัญชีเงินฝากของสถาบันการเงิน [๑๐] และข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศ และการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการทำธุรกรรมแบบพบเห็นลูกค้าต่อหน้าสำหรับธนาคาร [๑๑] โดยทั่วไปแล้วมี ๓ รูปแบบ ได้แก่ (๑) พบเห็นต่อหน้า (๒) ไม่พบเห็นต่อหน้า และ (๓) เสมือนพบเห็นต่อหน้า

๑๐.๑ พบเห็นต่อหน้า (Face-to-Face)

ผู้สมัครใช้บริการต้องแสดงตนพร้อมนำข้อมูลและเอกสารหลักฐานการแสดงตนยื่นต่อหน้าเจ้าพนักงานที่มีอำนาจหน้าที่รับผิดชอบและผ่านการฝึกอบรมที่ผู้พิสูจน์และยืนยันตัวตนกำหนดให้เป็นผู้ตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบันของข้อมูล เพื่อพิสูจน์ว่าเป็นบุคคลนั้นจริงและมีเพียงหนึ่งเดียว

๑๐.๒ ไม่พบเห็นต่อหน้า (Non Face-to-Face)

ผู้พิสูจน์และยืนยันตัวตนต้องจัดให้มีกระบวนการลงทะเบียนและพิสูจน์ตัวตนผ่านระบบดิจิทัลที่มีความน่าเชื่อถือ และมีมาตรการหรือระบบรักษาความมั่นคงปลอดภัย ในการตรวจสอบข้อมูลและหลักฐานของผู้สมัครใช้บริการเทียบเท่ากับการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า หรือเสมือนพบเห็นต่อหน้า เช่น การใช้เทคโนโลยีเพื่อพิสูจน์ความเป็นบุคคลและสังเกตพฤติกรรมผู้สมัครใช้บริการ (Liveness Detection) และเทคโนโลยีเปรียบเทียบข้อมูลชีวมิติของผู้สมัครใช้บริการ (Biometric Comparison) เพื่อพิสูจน์ว่าเป็นผู้สมัครใช้บริการรายนั้นจริงทดแทนการพบเห็นต่อหน้า ถ้าไม่สามารถสังเกตพฤติกรรมของผู้สมัครใช้บริการ ผู้พิสูจน์และยืนยันตัวตนต้องกำหนดกระบวนการหรือแนวทางการบริหารความเสี่ยงเพิ่มเติมเพื่อลดความเสี่ยงจากกรณีทุจริตต่าง ๆ ได้

๑๐.๓ เสมือนพบเห็นต่อหน้า (Supervised Remote)

ผู้พิสูจน์และยืนยันตัวตนต้องจัดให้มีกระบวนการลงทะเบียนและพิสูจน์ตัวตนผ่านระบบดิจิทัลที่มีความน่าเชื่อถือ และมีมาตรการหรือระบบรักษาความมั่นคงปลอดภัย ในการตรวจสอบข้อมูลและหลักฐานของผู้สมัครใช้บริการเทียบเท่ากับการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า รวมถึงจัดให้มีเจ้าพนักงานที่มีอำนาจหน้าที่รับผิดชอบและผ่านการฝึกอบรม ทำหน้าที่เฝ้าสังเกตและเข้าร่วมสนทนาออนไลน์กับผู้สมัครใช้บริการแบบถ่ายทอดสดตลอดเวลาของการลงทะเบียนและพิสูจน์ตัวตน เช่น การส่งผ่านวิดีโอที่มีความละเอียดสูงอย่างต่อเนื่อง (High Resolution Video Transmission)

ทั้งนี้ ต้องดำเนินการให้เป็นไปตามแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่อง การใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – การพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับบุคคลธรรมดาที่มีสัญชาติไทย และต้องบริหารความเสี่ยงที่เหมาะสมและสอดคล้องกับความเสี่ยงของบริการภาครัฐ ซึ่งการทำความรู้จักผู้ใช้บริการแบบไม่พบเห็นต่อหน้าและแบบเสมือนพบเห็นต่อหน้าอาจมีความเสี่ยงสูงกว่าแบบพบเห็นต่อหน้า ดังนั้นจึงต้องพิสูจน์ตัวตนในระดับที่เข้มข้นกว่า รวมถึงอาจมีวิธีการอื่น ๆ เพื่อช่วยบริหารความเสี่ยงที่อาจเกิดขึ้นได้

อนึ่ง เมื่อผู้ให้บริการภาครัฐพิจารณากลุ่มการให้บริการภาครัฐ ระดับความน่าเชื่อถือของไอเดนทิตี และรูปแบบการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลสำหรับบริการภาครัฐแล้ว ให้ผู้ให้บริการภาครัฐและผู้พิสูจน์และยืนยันตัวตนกำหนดข้อตกลงร่วมกันในการลงทะเบียนและพิสูจน์ตัวตนทางดิจิทัลสำหรับบริการภาครัฐและปฏิบัติตามข้อตกลงนั้น

บรรณานุกรม

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

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

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

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

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

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

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

[๘] ประมวลกฎหมายอาญา.

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

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

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

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