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

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 เพื่อปรับปรุงให้มาตรฐานรัฐบาลดิจิทัลฉบับนี้มีความครบถ้วนสมบูรณ์ สามารถนำไปปรับใช้ในทางปฏิบัติได้

มาตรฐานรัฐบาลดิจิทัล ว่าด้วยแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ – ภาพรวม ฉบับนี้ จัดทำขึ้นโดยคณะกรรมการจัดทำร่างมาตรฐาน ข้อกำหนดและหลักเกณฑ์ 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

(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

สารบัญภาพ

ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล

เรื่อง มาตรฐานและหลักเกณฑ์การจัดทำกระบวนการและการดำเนินงานทางดิจิทัล ว่าด้วยเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สำหรับบุคคลธรรมดาที่มีสัญชาติไทย

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

เพื่อให้การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัลเป็นไปตามวัตถุประสงค์ดังกล่าวข้างต้น โดยที่พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ มาตรา ๑๒ (๒) กำหนดให้หน่วยงานของรัฐจัดทำกระบวนการหรือการดำเนินงานทางดิจิทัลเพื่อการบริหารราชการแผ่นดินและการให้บริการประชาชน กระบวนการหรือการดำเนินงานทางดิจิทัลนั้นต้องทำงานร่วมกันได้ตามมาตรฐาน ข้อกำหนด และหลักเกณฑ์ที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด เพื่อให้มีความสอดคล้องและเชื่อมโยงระหว่างหน่วยงานของรัฐแห่งอื่นได้ 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 คณะกรรมการพัฒนารัฐบาลดิจิทัลในคราวการประชุมครั้งที่ ๒/๒๕๖๔ วันที่๑๓ 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 ซึ่งสามารถใช้ระบุตัวบุคคลในบริบทที่กำหนด และสามารถใช้ทำธุรกรรมอิเล็กทรอนิกส์

"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 หรือกลุ่มข้อมูล ที่เชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตน

"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) ให้ความสำคัญและบริหารความเสี่ยงให้เหมาะสมกับระดับความเสี่ยงของบริการภาครัฐ โดยพิจารณาถึงผลกระทบที่อาจเกิดขึ้น เพื่อกำหนดวิธีการบรรเทาความเสียหายที่อาจเกิดขึ้น

ผู้พิสูจน์และยืนยันตัวตน ผู้ให้บริการภาครัฐ และแหล่งให้ข้อมูลที่น่าเชื่อถือที่เป็นหน่วยงานของรัฐ ให้จัดทำธรรมาภิบาลข้อมูลภาครัฐและดำเนินการให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐที่เกี่ยวข้องกับกระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐด้วย

หมวด ๒
การพิสูจน์และยืนยันตัวตนทางดิจิทัล

ข้อ ๔ ให้ผู้พิสูจน์และยืนยันตัวตนดำเนินการ ดังต่อไปนี้

(๑) กำหนดรูปแบบของการพิสูจน์และยืนยันตัวตนทางดิจิทัล และจัดสรรบุคลากร ระบบ เทคโนโลยีที่จำเป็น ให้สอดคล้องกับระดับความน่าเชื่อถือ

(๒) กำหนดนโยบายและกระบวนการปฏิบัติงานภายในที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ชัดเจนเป็นลายลักษณ์อักษร โดยต้องทบทวน สื่อสาร ทำความเข้าใจ สร้างความตระหนักให้กับเจ้าหน้าที่ที่ได้รับการฝึกอบรมหรือบุคลากรที่เกี่ยวข้องให้เห็นถึงความสำคัญ และปฏิบัติตามนโยบายและกระบวนการปฏิบัติงานภายในหรือหน่วยงานกำกับดูแลที่เกี่ยวข้อง รวมถึงต้องสื่อสารทำความเข้าใจและให้ความรู้กับผู้ใช้บริการด้วย

(๓) กรณีที่ผู้พิสูจน์และยืนยันตัวตนเป็นหน่วยงานของรัฐให้ดำเนินการตามข้อกำหนดการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามมาตรฐานและหลักเกณฑ์นี้ หากผู้พิสูจน์และยืนยันตัวตนเป็นหน่วยงานของเอกชนให้ดำเนินการตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

(๔) จัดให้มีการขอความยินยอมของผู้สมัครใช้บริการ โดยต้องแจ้งวัตถุประสงค์ของการจัดเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลด้วย

(๕) จัดให้มีการแสดงตนและรวบรวมข้อมูลเพื่อระบุตัวตนที่จำเป็นจากผู้สมัครใช้บริการ เพื่อแยกแยะว่าไอเดนทิตีของผู้สมัครใช้บริการมีเพียงหนึ่งเดียว 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 รวมถึงกำหนดเงื่อนไขให้สอดคล้องตามข้อกำหนดในแต่ละระดับความน่าเชื่อถือตามกลุ่มให้บริการภาครัฐ และแจ้งให้ทราบล่วงหน้า

ข้อ ๖ ให้แหล่งให้ข้อมูลที่น่าเชื่อถือตรวจสอบข้อมูลหรือสถานะของหลักฐานแสดงตนของผู้สมัครใช้บริการตามการร้องขอจากผู้พิสูจน์และยืนยันตัวตน และส่งผลการตรวจสอบข้อมูลกลับไปยังผู้พิสูจน์และยืนยันตัวตน

บทเฉพาะกาล

ข้อ ๗ ในระยะเริ่มแรก มิให้นำมาตรฐานและหลักเกณฑ์ตามประกาศนี้มาใช้บังคับกับผู้พิสูจน์และยืนยันตัวตน ผู้ให้บริการภาครัฐ และแหล่งให้ข้อมูลที่น่าเชื่อถือ จนกว่าจะพ้นกำหนดสองปีนับแต่วันที่ประกาศนี้มีผลใช้บังคับ

ประกาศ ณ วันที่ ๑๖ กันยายน ๒๕๖๔

(นายตอน ปรมัตถ์วินัย)
รองนายกรัฐมนตรี
ประธานกรรมการพัฒนารัฐบาลดิจิทัล

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) เป็นการอธิบายข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตนในการยืนยันตัวตนของผู้ใช้บริการที่ประสงค์จะทำธุรกรรมออนไลน์ด้วยดิจิทัลไอดี ตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

๔. แบบจำลองดิจิทัลไอดี (Digital Identity Model)

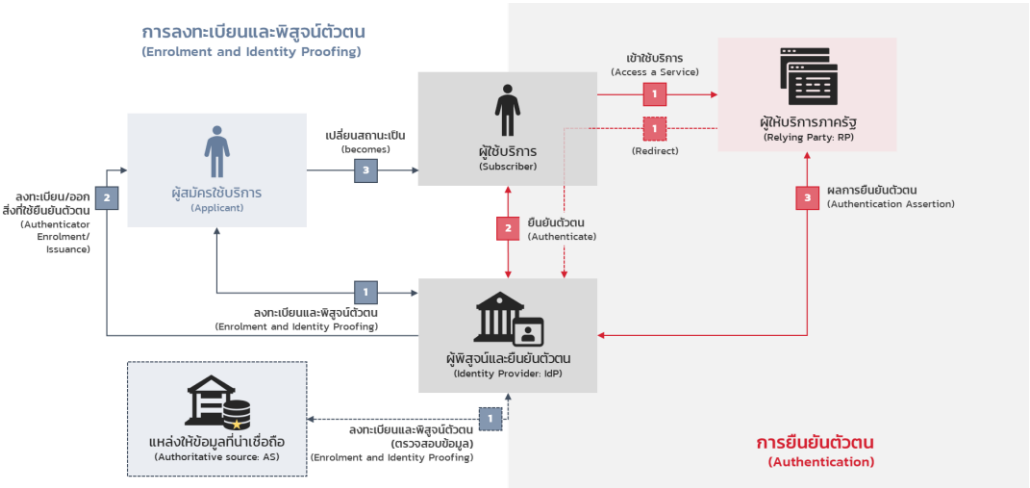
๔.๑ ภาพรวม (Overview)

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

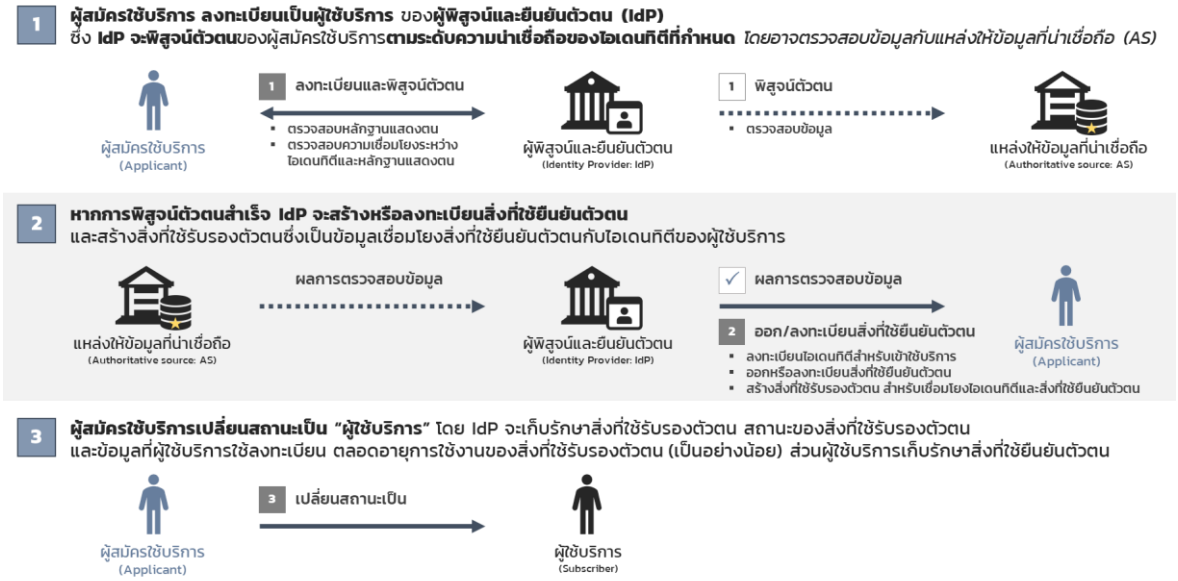
๔.๒.๓.๒ ไม่พบเห็นต่อหน้า (Non Face-to-Face)

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

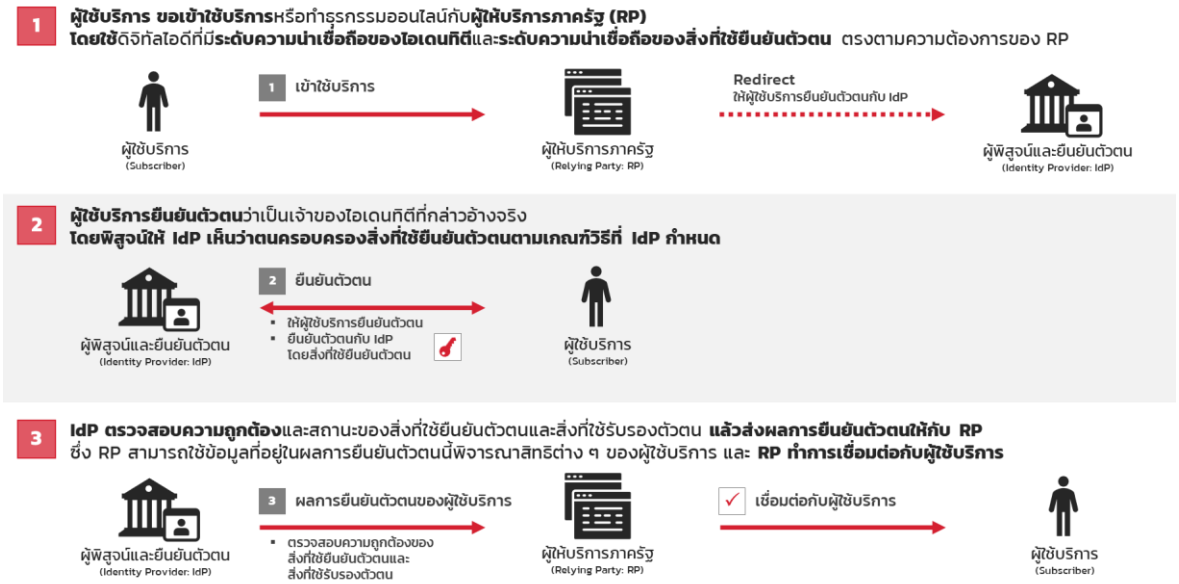
(๒) มีอย่างน้อยหนึ่งปัจจัยที่ปกป้องข้อมูลลับซึ่งเป็นอีกปัจจัยหนึ่ง เช่น ใช้อุปกรณ์ฮาร์ดแวร์ที่มีวิธีการเข้ารหัสลับ (สิ่งที่ผู้ใช้บริการมี) และใช้ลายนิ้วมือ (สิ่งที่ผู้ใช้บริการเป็น) ในการเข้าถึงอุปกรณ์ดังกล่าวนั้น เพื่อยืนยันตัวตน

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

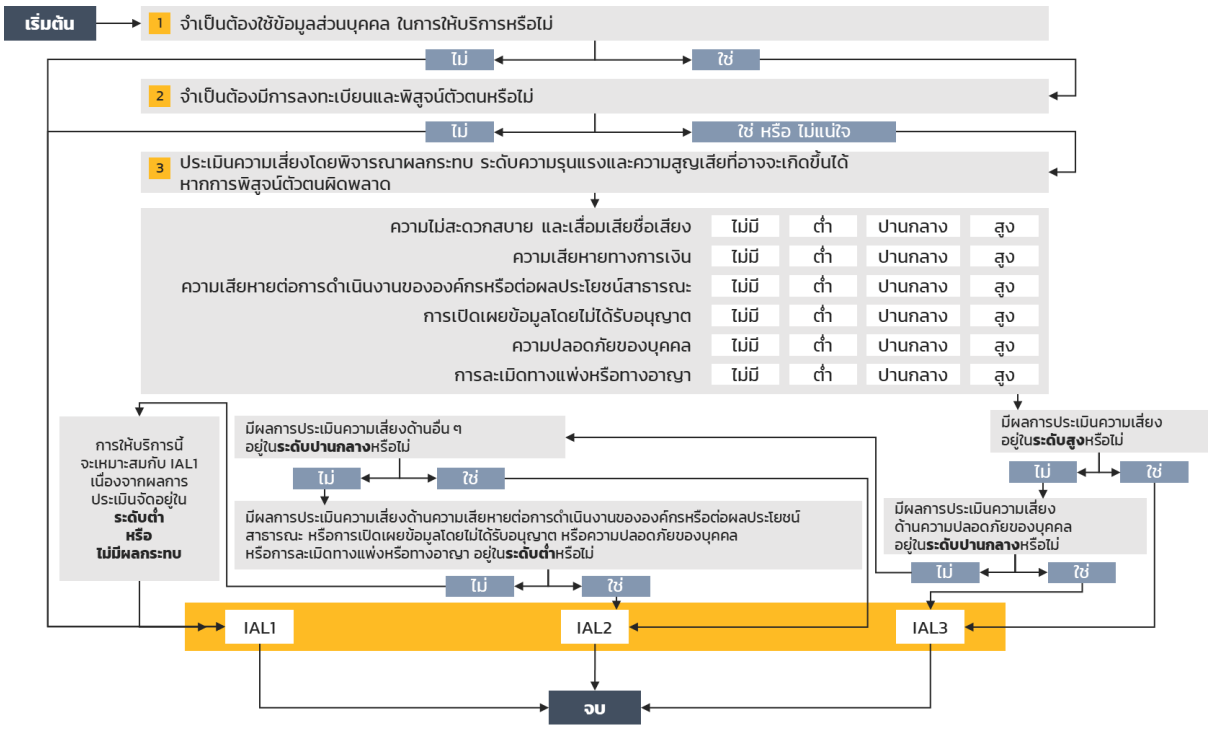
จากนั้น พิจารณาความหมายของแต่ละระดับความเสี่ยง ดังตารางที่ ๕

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

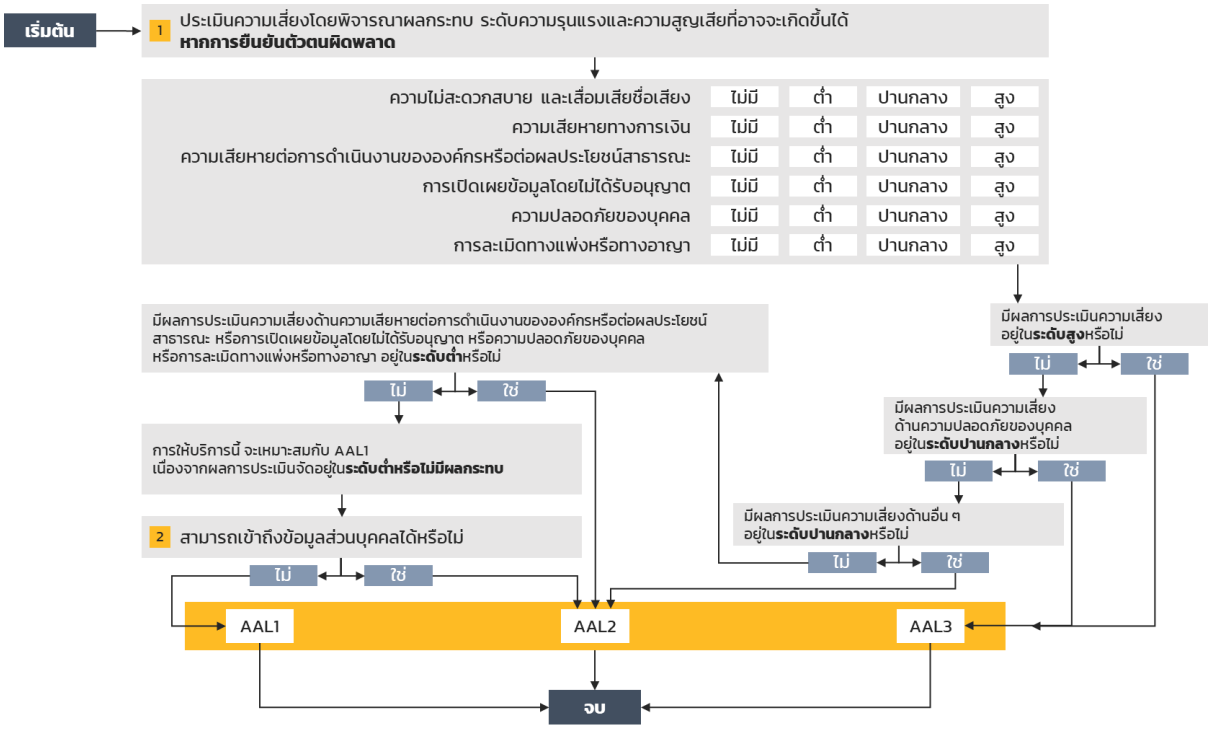
(๕) กรณีที่นอกเหนือจากนี้ ให้กำหนดเป็น **ระดับ** IAL1

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.