Mobile ID บทบาทใหม่ในการพัฒนา Digital ID ของไทย

MOBILE ID: A SIGNIFICANT ROLE IN THE DEVELOPMENT OF DIGITAL ID IN THAILAND

จิตสถา ศรีประเสริฐสุข

Chitsata Sriprasertsuk

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
กรุงเทพฯ 10400

Office of the National Broadcasting and Telecommunications Commission,
Bangkok 10400 Thailand

Corresponding E-mail : chitsata@gmail.com

บทคัดย่อ

เทคโนโลยีดิจิทัลมีความก้าวหน้าและมีนวัตกรรมใหม่พัฒนาอย่างต่อเนื่อง ความต้องการและพฤติกรรมของผู้บริโภคมีการปรับเปลี่ยนไปสู่การใช้บริการในรูปแบบดิจิทัลที่สะดวกสบายมากขึ้น ส่งผลให้การระบุตัวตนในรูปแบบดิจิทัล หรือ Digital Identity (Digital ID) เริ่มเข้ามามีบทบาทอย่างแพร่หลายในระดับสากลอันเป็นผลมาจากประโยชน์ทั้งทางตรงและทางอ้อมต่อเศรษฐกิจและสังคม ประเทศไทยได้มีการพัฒนานโยบายที่เกี่ยวข้องกับ Digital ID ขึ้นในหลากหลายบทบาท ทั้งการกำหนดทิศทาง ออกกฎหมายและกฎระเบียบ รวมถึงการพัฒนาและประยุกต์ใช้เทคโนโลยีที่จำเป็น และการบูรณาการความร่วมมือจากหลายภาคส่วน หนึ่งในงานยุคใหม่ที่สำนักงาน กสทช. ได้ให้ความสำคัญคือ การพัฒนาและส่งเสริมการให้บริการ Mobile ID เพื่อเป็นหนึ่งในทางเลือกของ Digital ID ที่ประชาชนเลือกใช้ ซึ่งมีคุณลักษณะเฉพาะตัวและโดดเด่น จึงนับเป็นความท้าทายใหม่ที่สำนักงาน กสทช. ได้สร้างบทบาทในการเป็นผู้ริเริ่มและผู้สนับสนุนให้อุตสาหกรรมโทรคมนาคมนำจุดแข็งและศักยภาพที่เด่นชัดไปสร้างมูลค่าเพิ่มในการให้บริการประชาชนในโลกยุคดิจิทัล อีกทั้งเป็นผู้ประสานความร่วมมือในระดับหน่วยงานนโยบาย เพื่อร่วมพิจารณาทิศทางการส่งเสริม การกำกับดูแล และการบูรณาการการให้บริการ Digital ID ของประเทศ ให้มีการพัฒนาและเติบโตด้วยความน่าเชื่อถือ มีความปลอดภัยในการใช้งาน และก่อประโยชน์ต่อสังคมและเศรษฐกิจ

คำสำคัญ: การพิสูจน์และยืนยันตัวตนทางดิจิทัล ระบบการพิสูจน์และยืนยันตัวตนด้วยรูปแบบบัตรประจำตัวอิเล็กทรอนิกส์บนโทรศัพท์เคลื่อนที่ การระบุตัวตนในรูปแบบดิจิทัล

Abstract

Due to the developed digital technology and advanced innovations, demands and behaviors have shifted towards digital services. Consequently, Digital Identity has begun to play a prevalent role globally, for it provides both direct and indirect benefits to the economy and society. In Thailand, there have been developed policies related to Digital ID in various roles, such as issuing guidelines, the legislation of rules and regulations including the development and application of necessary technologies, and the integration of cooperation from many sectors. The Office of the NBTC has given importance to the development and promotion of the Mobile ID Platform service, which is unique and distinctive, to be one of the digital ID alternatives. It is, therefore, a new challenge for the Office of the NBTC to initiate and advocate the telecommunication industry to bring strengths and potential to generate added value in services for people in the digital world. Moreover, the Office of the NBTC would also act as coordinator to collaborate the promotion, the regulation, and the integration among the Digital ID platforms to evolve with credibility and security which allow us to achieve the highest potential of Digital ID services. Therefore, greater advantages would be created for society and the economy.

Keywords: Digital ID, Mobile ID, Digital Identification

1. บทนำ

ในยุคที่มีการเปลี่ยนแปลงทางเทคโนโลยีอย่างรวดเร็ว เราพบเห็นการเปลี่ยนแปลงพฤติกรรมการใช้ชีวิตของประชาชน และการเปลี่ยนแปลงรูปแบบการให้บริการในโลกยุคดิจิทัล โดยมีการพัฒนาการให้บริการในรูปแบบใหม่ ๆ ที่ทันสมัยขึ้นทั้งในรูปแบบที่พบเห็นหน้ากันระหว่างผู้ใช้บริการและผู้ให้บริการ และรูปแบบออนไลน์ที่มีการเติบโตอย่างก้าวกระโดด ในระดับสากลได้นิยมนำ Digital Identity[1] หรือ Digital ID มาใช้ระบุตัวตนของผู้ใช้งาน เพื่อให้การให้บริการและการใช้บริการในยุคดิจิทัลมีความน่าเชื่อถือ ตรวจสอบได้ ปลอดภัย และลดต้นทุนของผู้ให้บริการและการใช้ชีวิตของประชาชน จากการใช้ประโยชน์ Digital ID นั้น รายงานของ McKinsey Global Institute (2019) กล่าวไว้ว่า ภายในปี พ.ศ. 2573 Digital ID จะมีศักยภาพ

[1] Digital Identity คือ อัตลักษณ์ (identity) ที่ถูกรวบรวมและบันทึกในรูปแบบดิจิทัล ซึ่งใช้บ่งบอกหรือจำแนกบุคคลในการทำธุรกรรมอิเล็กทรอนิกส์ นิยามระบุในข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ขมธอ.18-2564 ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน โดยสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์

ในการสร้างมูลค่าทางเศรษฐกิจเทียบเท่ากับร้อยละ 6 ของผลิตภัณฑ์มวลรวมภายในประเทศ (Gross Domestic Product: GDP) ในประเทศเศรษฐกิจเกิดใหม่ (Emerging economies) และร้อยละ 3 ในประเทศที่มีระบบเศรษฐกิจเติบโตเต็มที่ (Mature economies) โดยตัวอย่างที่มีการเติบโตและเกิดผลประโยชน์ต่อเศรษฐกิจและสังคมอย่างมีนัยสำคัญในประเทศต่าง ๆ ได้แก่ การใช้งาน Digital ID ในการใช้บริการด้านการธนาคาร การจ้างงาน การจดแจ้งสิทธิ์ในที่ดินเกษตรกรรม การศึกษา และการบริหารจัดการเพื่อลดต้นทุนและประหยัดเวลาของภาคบริการ เป็นต้น

สำหรับประเทศไทยปัจจุบันมีความพร้อมที่จะพัฒนาให้เกิดการให้บริการ Digital ID ไม่ว่าจะเป็นการมีกฎหมายที่รองรับเรื่องนี้แล้ว มีการเตรียมการด้านกฎหมายและกฎระเบียบเพิ่มเติมที่จะบังคับใช้อนาคตอันใกล้ รวมทั้งมีการกำหนดทิศทางด้านนโยบายที่เริ่มจะมีความชัดเจนมากขึ้น ในขณะเดียวกันเทคโนโลยีที่จะใช้เพื่อให้บริการ Digital ID ก็มีความน่าเชื่อถือมากขึ้นในระดับสากล และที่สำคัญประชาชนก็มีความพร้อมที่จะใช้เทคโนโลยีและบริการใหม่ ๆ ที่จะทำให้การใช้ชีวิตมีความสะดวกสบายมากขึ้น Mobile ID จึงเป็น Digital ID ประเภทหนึ่งที่กำลังเข้ามามีบทบาทในการให้บริการกับประชาชน ในบทความนี้จึงได้นำเสนอที่มาของแนวคิดในการดำเนินงานของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) ซึ่งมีความเชื่อมโยงกับการเติบโตและพัฒนาการให้บริการของอุตสาหกรรมโทรคมนาคม กฎระเบียบที่เกี่ยวข้องที่มีส่วนสำคัญต่อการออกแบบและพัฒนา Mobile ID Platform รูปแบบการดำเนินงานที่เริ่มต้นจากการทดสอบทดลอง (Sandbox) ไปสู่ทิศทางในอนาคต รวมทั้งมุมมองของการพัฒนา Mobile ID ที่จะสนับสนุนการให้บริการ Digital ID ของประเทศไทย

2. วัตถุประสงค์

เพื่อนำเสนอบทบาทของสำนักงาน กสทช. ในการดำเนินงานและผลักดันเรื่อง Mobile ID เพื่อให้มีความเข้าใจในที่มาและมุมมองการพัฒนางานในอนาคต รวมทั้งนำเสนอบทบาทและความสัมพันธ์ของ Mobile ID ที่มีต่อทิศทางการพัฒนา Digital ID ของประเทศไทย

3. วิธีการศึกษา

ศึกษาเอกสารที่เกี่ยวข้อง เช่น เอกสารด้านกฎหมาย เอกสารด้านมาตรฐานทางเทคนิค รายงานวิจัย และข้อมูลของต่างประเทศ ประกอบกับการประมวลผลจากประสบการณ์ที่ได้รับจากการปฏิบัติงานจริง และจากการแลกเปลี่ยนความคิดเห็นกับหน่วยงานต่าง ๆ ที่เกี่ยวข้องในโอกาสต่าง ๆ

4. ผลการศึกษา

เกิดความชัดเจนในทิศทางการพัฒนา Mobile ID ของอุตสาหกรรมโทรคมนาคม และบทบาทของสำนักงาน กสทช. ในการร่วมผลักดันการพัฒนาและการเติบโตในการให้บริการ Digital ID ของประเทศไทย ดังนี้

4.1 การลงทะเบียนซิมผู้ใช้บริการโทรศัพท์เคลื่อนที่สู่ Mobile ID

ที่มาของแนวคิดและแนวทางการทำงานของสำนักงาน กสทช. ในการผลักดันเรื่อง Mobile ID นั้น มาจากรากฐานความสำเร็จของการขับเคลื่อนนโยบายเรื่องการลงทะเบียนซิมผู้ใช้บริการโทรศัพท์เคลื่อนที่ หรือโทรศัพท์มือถือ เมื่อปี พ.ศ. 2557 ที่มีการออกนโยบายให้ผู้ให้บริการโทรศัพท์เคลื่อนที่ต้องลงทะเบียนซิมและยืนยันตัวตนผู้ใช้บริการก่อนมีการเปิดใช้งานเลขหมายหรือเบอร์โทรศัพท์เคลื่อนที่ และได้กำหนดนโยบายให้ประชาชนที่ใช้งานเลขหมายที่ยังไม่เคยลงทะเบียนให้มาลงทะเบียนให้ครบถ้วน ทำให้ในปี พ.ศ. 2558 ทุกเลขหมายโทรศัพท์เคลื่อนที่มีชื่อผู้ใช้บริการ ถือเป็นยุคเริ่มต้นของการบริหารจัดการการลงทะเบียนซิมในรูปแบบดิจิทัล หรือมีการจัดเก็บข้อมูลบัตรประจำตัวประชาชนและข้อมูลผู้ใช้บริการในรูปแบบอิเล็กทรอนิกส์ (การลงทะเบียนซิมด้วย “แอปพลิเคชัน 2 แชะ”) แทนการจัดเก็บสำเนาบัตรประชาชนในรูปแบบกระดาษที่เคยดำเนินการมาตั้งแต่อดีต ในช่วงเวลาดังกล่าวถือเป็นการเริ่มต้นของ กสทช. และสำนักงาน กสทช. ในการพยายามจัดระเบียบอุตสาหกรรมโทรคมนาคมให้มีฐานข้อมูลผู้ใช้บริการในทุกเลขหมาย เพื่อให้ผู้ใช้บริการได้รับการคุ้มครองสิทธิ์ในการใช้บริการในฐานะเจ้าของเลขหมาย อีกทั้งข้อมูลผู้ใช้บริการยังสามารถใช้สนับสนุนหน่วยงานภาครัฐในการดูแลประชาชนและสังคมให้ปลอดภัย เช่น กรณีเกิดมีการนำเลขหมายโทรศัพท์เคลื่อนที่ไปใช้ในทางที่มิชอบ ก็จะสามารถหาผู้กระทำความผิดมาลงโทษได้ถูกต้องและเป็นไปโดยง่ายขึ้นกว่าในอดีต

การบริหารจัดการทั้งการออกกฎเกณฑ์ของ กสทช. การกำกับดูแลของสำนักงาน กสทช. และการปฏิบัติหน้าที่ของผู้ประกอบการมีการพัฒนาอย่างต่อเนื่องจนในปี พ.ศ. 2561 ได้มีการนำเทคโนโลยีการตรวจสอบอัตลักษณ์บุคคล (Biometric) มาพัฒนาใช้สำหรับการลงทะเบียนซิมการ์ด (แอปพลิเคชัน “2 แชะ อัตลักษณ์”) เพื่อลดปัญหาการแอบอ้างและปลอมแปลงการนำบัตรประจำตัวประชาชนผู้อื่นมาใช้ลงทะเบียนซิมการ์ด โดยได้นำระบบการตรวจสอบใบหน้า (Facial recognition หรือ Face comparison) มาใช้ตรวจสอบและยืนยันตัวบุคคลว่า ผู้ที่ประสงค์จะลงทะเบียนซิมเป็นเจ้าของบัตรประจำตัวประชาชนที่นำมาใช้อ้างอิงในการลงทะเบียนซิมการ์ดหรือไม่ (กรณีชาวต่างชาติใช้หนังสือเดินทาง) ก่อนจะมีการอนุญาตให้ลงทะเบียนและจัดเก็บข้อมูลผู้ใช้บริการและเปิดใช้งานซิมการ์ดต่อไป ช่วงเวลาดังกล่าวถือเป็นยุคของการพัฒนาให้เกิดการจัดเก็บข้อมูลผู้ใช้บริการให้ถูกต้องมากขึ้นมาเป็นลำดับ และเป็นการริเริ่มนำเทคโนโลยีด้านการตรวจสอบอัตลักษณ์บุคคลมาใช้ครั้งแรกในวงการโทรคมนาคม

เมื่ออุตสาหกรรมโทรคมนาคมเริ่มพัฒนาการจัดเก็บข้อมูลผู้ใช้บริการโทรศัพท์เคลื่อนที่อย่างต่อเนื่อง ประกอบกับเลขหมายโทรศัพท์เคลื่อนที่กลายเป็นสิ่งที่ใช้อ้างอิงตัวตนในการใช้บริการ โดยเฉพาะในโลกออนไลน์ ส่งผลให้สำนักงาน กสทช. มองเห็นโอกาสในการนำฐานข้อมูลผู้ใช้บริการโทรศัพท์เคลื่อนที่ไปใช้ประโยชน์มากขึ้น เช่น กรณีการให้บริการ Prompt Pay ของภาคธนาคารที่จะมีการตรวจสอบความเป็นเจ้าของเลขหมายโทรศัพท์ก่อนประชาชนมีสิทธิ์เข้าใช้บริการ หรือแม้แต่ภาคโทรคมนาคมเองก็ตามที่สำนักงาน กสทช. ได้นำประโยชน์จากเรื่องนี้ไปพัฒนาแอปพลิเคชัน 3 ชั้น (ตรวจ แจ้ง ล็อก)[2] โดยร่วมกับผู้ประกอบการโทรศัพท์เคลื่อนที่ในการบูรณาการและจัดทำระบบร่วมกันเพื่อสร้างเครื่องมือทางดิจิทัลให้กับผู้ใช้บริการให้สามารถควบคุมดูแลเบอร์โทรศัพท์ที่ได้ลงทะเบียนซิมไว้ในชื่อตนเอง และป้องกันการถูกลักลอบนำชื่อของตนไปลงทะเบียนซิมโดยบุคคลอื่น

จากจุดเริ่มต้นของการกำกับดูแลเรื่องการลงทะเบียนซิมการ์ดนี้ และจากตัวอย่างสองเรื่องที่โดดเด่นจากการใช้ประโยชน์ของฐานข้อมูลผู้ใช้บริการโทรศัพท์เคลื่อนที่ ทำให้สำนักงาน กสทช. ต้องเปิดมุมมองใหม่ต่อเนื่องเพื่อสนับสนุนให้อุตสาหกรรมโทรคมนาคมนำจุดเด่นและข้อได้เปรียบของตนไปสนับสนุนภาคส่วนอื่นเพิ่มเติม รวมถึงการเปิดธุรกิจบริการใหม่ ๆ ที่สร้างมูลค่าเพิ่มให้กับประชาชนผู้ใช้บริการได้นอกเหนือไปจากการให้บริการพื้นฐานด้านโทรคมนาคม เช่น บริการเสียงและอินเทอร์เน็ต ดังนั้น การส่งเสริมและผลักดันการดำเนินงานเรื่อง Mobile ID ให้เป็นทางเลือกของ Digital ID ของประเทศจึงเป็นเป้าหมายหนึ่ง

ภาพที่ 1 พัฒนาการของการลงทะเบียนซิมการ์ดและการนำประโยชน์ของฐานข้อมูลการลงทะเบียนซิมการ์ดไปใช้งาน

[2] แอปพลิเคชัน 3 ชั้น (ตรวจ แจ้ง ล็อก) เป็นแอปพลิเคชันที่รักษาสิทธิ์ผู้ใช้บริการ โดย 1) สามารถตรวจสอบได้ว่ามีการลงทะเบียนซิมโดยใช้ชื่อของตนเองไปกี่เบอร์และอยู่ค่ายไหนบ้าง (ตรวจ) 2) หากเจอเบอร์แปลกปลอมที่ในอดีตอาจเคยมีคนนำบัตรประจำตัวประชาชนของตนไปแอบอ้างลงทะเบียนซิมก็จะสามารถแจ้งให้ผู้ประกอบการยกเลิกเบอร์ได้ หรือแม้แต่หากตรวจสอบพบว่าเบอร์ของตนหายไปก็จะได้แจ้งให้ผู้ประกอบการตรวจสอบให้ (แจ้ง) และ 3) ที่สำคัญผู้ใช้บริการสามารถล็อกเพื่อป้องกันการเปิดเบอร์เพิ่มโดยตนไม่รู้ตัว (ล็อก) เช่น อาจมีผู้ไม่หวังดีแอบนำบัตรประชาชนของตนไปลงทะเบียนซิมเพื่อนำไปใช้ในทางที่มิชอบ

4.2 ทำไมต้องเป็น Mobile ID

ในยุคปัจจุบันที่มีการเจริญเติบโตของโลกสื่อสารโทรคมนาคมอย่างต่อเนื่อง โทรศัพท์เคลื่อนที่กลายเป็นปัจจัยที่ห้าของประชาชนคนไทยหรือแม้แต่ในสังคมโลก ประเทศไทยเรามีประชากรประมาณ 67 ล้านคน แต่มีเลขหมายโทรศัพท์เคลื่อนที่ที่เปิดใช้งานอยู่ 117 ล้านเลขหมาย แสดงให้เห็นว่าแทบจะทุกคนมีโทรศัพท์เคลื่อนที่ใช้และบางคนมีมากกว่าหนึ่งเลขหมาย ทุกคนคงยอมรับว่าโทรศัพท์เคลื่อนที่กลายเป็นสิ่งที่จำเป็นหรือเป็นสิ่งที่ทุกคนต้องการนำติดตัวไปด้วยทุกที่ทุกเวลา และมีความสำคัญไม่น้อยไปกว่าการพกกระเป๋าเงินหรือบัตรประจำตัวประชาชน ในขณะเดียวกันเบอร์โทรศัพท์เคลื่อนที่กลายเป็นสิ่งที่นิยมใช้ในการอ้างอิงตัวบุคคลสำหรับการใช้บริการของทั้งภาครัฐและเอกชน บางบริการใช้แค่เบอร์โทรศัพท์ บางบริการใช้เบอร์ควบคู่ไปกับบัตรประจำตัวประชาชน อย่างไรก็ตาม การให้บริการต่าง ๆ ของภาคเอกชนมักใช้เลขหมายโทรศัพท์เคลื่อนที่เพียงอย่างเดียวในการอ้างอิงตัวตนและการยืนยันตัวตน โดยเฉพาะบริการที่อยู่ในโลกออนไลน์ หรือการให้บริการผ่านแอปพลิเคชันต่าง ๆ ยิ่งทำให้เห็นการเติบโตของการใช้เลขหมายโทรศัพท์เคลื่อนที่ในการอ้างอิงตัวตนนั้นเติบโตอย่างก้าวกระโดด

เมื่อโทรศัพท์เคลื่อนที่กลายเป็นสิ่งสำคัญสำหรับชีวิตประจำวัน เมื่ออุตสาหกรรมโทรคมนาคมสามารถนำฐานข้อมูลผู้ใช้บริการโทรศัพท์เคลื่อนที่ซึ่งเป็นผลมาจากนโยบายการลงทะเบียนซิมของ กสทช. มาใช้ให้เกิดประโยชน์และสร้างมูลค่าเพิ่มในการให้บริการกับประชาชนได้ และเมื่อเกิดความนิยมในการใช้เบอร์โทรศัพท์เป็นสิ่งอ้างอิงตัวบุคคล Mobile ID ซึ่งคือ “Digital ID ประเภทหนึ่งที่ใช้ระบุตัวบุคคลและเชื่อมโยงกับความเป็นเจ้าของเบอร์โทรศัพท์และเจ้าของบัตรประจำตัวประชาชน” จึงเป็นทางเลือกหนึ่งของ Digital ID ของประเทศไทย ที่จะอำนวยความสะดวกสบายให้กับประชาชนในการเข้าใช้บริการและทำธุรกรรมของภาครัฐและเอกชนได้อย่างหลากหลาย แพร่หลาย เป็นไปอย่างปลอดภัย และที่สำคัญสามารถคุ้มครองข้อมูลส่วนบุคคลได้

ในแง่ประโยชน์จากการใช้งาน Mobile ID นั้น ลองจินตนาการดูว่า จะดีเพียงใดหาก Mobile ID สามารถนำมาใช้แทนบัตรประจำตัวประชาชนเพื่อติดต่อใช้บริการในสถานที่ต่าง ๆ เราก็จะไม่ต้องกังวลว่าใครจะเอาข้อมูลส่วนบุคคลบนหน้าบัตรประจำตัวประชาชนของเราไปทำสำเนาใช้ในทางที่มิชอบ จะดีเพียงใดหากในการใช้บริการต่าง ๆ ทั้ง ณ จุดให้บริการที่พบเห็นหน้ากันและในโลกออนไลน์จะสามารถมีการยืนยันได้จริงว่าผู้ใช้บริการเป็นเจ้าของหมายเลขโทรศัพท์และเป็นเจ้าของบัตรประจำตัวประชาชนที่ใช้อ้างอิง นั่นหมายความว่า ผู้ให้บริการก็มั่นใจได้ว่าผู้ใช้บริการคนนั้นเป็นตัวตนจริง ไม่มีการปลอมแปลง และยังมีข้อมูลหมายเลขโทรศัพท์ที่อ้างอิงความเป็นเจ้าของได้ด้วย และในแง่ประชาชนผู้ใช้บริการเองก็มั่นใจว่าหากผู้ให้บริการมีกระบวนการในการพิสูจน์และยืนยันตัวตนที่น่าเชื่อถือ เราก็จะไม่ถูกนำหมายเลขโทรศัพท์ไปแอบอ้างใช้หรือถูกนำบัตรประจำตัวประชาชนของเราไปลักลอบใช้หรือมีการปลอมแปลงนำไปใช้งานโดยมิชอบ

4.3 หลักการและแนวคิดของ Mobile ID Platform

ด้วยการดำเนินงานในเรื่องนี้เป็นเรื่องใหม่ของประเทศไทย และเป็นเรื่องใหม่ของอุตสาหกรรมโทรคมนาคม ประกอบกับเป็นการดำเนินงานที่มีการกำหนดมาตรฐานในเรื่องการพิสูจน์และยืนยันตัวตน โดยสำนักงานคณะกรรมการธุรกรรมอิเล็กทรอนิกส์แห่งชาติ (สพธอ.) สำนักงาน กสทช. จึงได้เริ่มต้นโครงการในลักษณะการทดสอบทดลองร่วมกับผู้ที่สนใจและมีศักยภาพ โดยได้รับความร่วมมือจากผู้ให้บริการโทรศัพท์เคลื่อนที่ทุกเครือข่าย รวมทั้งหน่วยงานภาครัฐและเอกชนเข้าร่วมทดสอบทดลองรวมทั้งสิ้น 14 หน่วยงาน โดยมีการจัดทำบันทึกความเข้าใจ (Memorandum of Understanding: MOU) และจัดตั้งคณะทำงานร่วมกัน และมี สพธอ. เข้าร่วมในคณะทำงานเพื่อให้คำปรึกษาด้วย

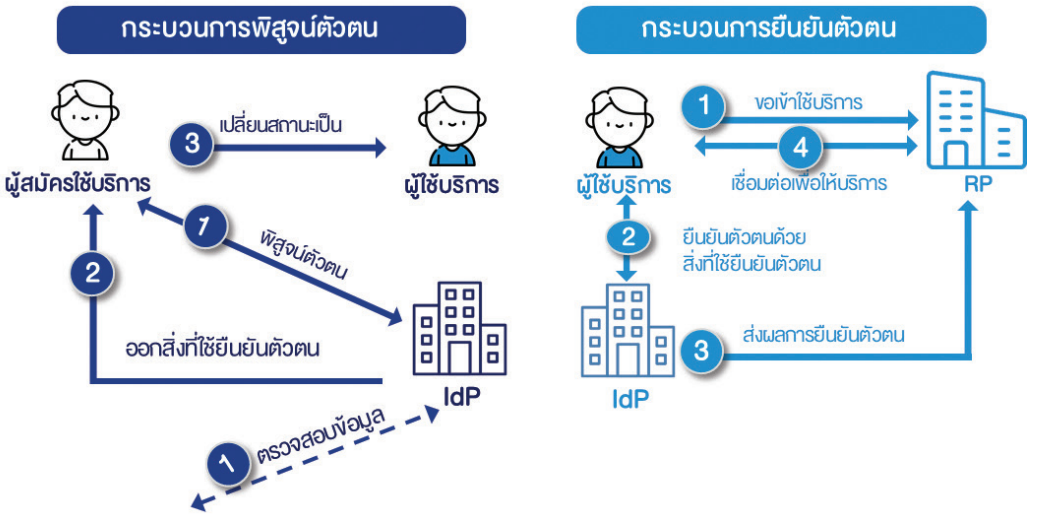
ก่อนจะอธิบายเรื่องโครงสร้างการทำงานของ Mobile ID นั้น จำเป็นต้องเข้าใจโครงสร้างความสัมพันธ์กับผู้ที่เกี่ยวข้องหลักที่เป็นองค์ประกอบในการให้บริการ Digital ID และกระบวนการทำงานของ Digital ID ตามมาตรฐานที่ สพธอ. กำหนดไว้[3] สรุปดังนี้

ตารางที่ 1 องค์ประกอบของผู้ที่เกี่ยวข้องกับการให้บริการ Digital ID

องค์ประกอบ	นิยาม/บทบาท	หมายเหตุ
ผู้พิสูจน์และยืนยันตัวตน (Identity Provider: IdP)	หน่วยงานที่ให้บริการแก่บุคคลภายนอกเกี่ยวกับการพิสูจน์ตัวตน การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน หรือการยืนยันตัวตน	สพธอ. กำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL) [ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของบุคคล]
ผู้อาศัยการยืนยันตัวตน (Relying Party: RP)	บุคคลหรือหน่วยงานที่พึ่งพาอาศัยผลการยืนยันตัวตนจาก IdP หรือสิ่งที่ใช้ยืนยันตัวตนที่ผู้ใช้บริการมีอยู่ก่อนแล้ว ในการตัดสินใจที่จะให้บริการธุรกรรมหรือให้สิทธิในการเข้าใช้ระบบ	สพธอ. กำหนดระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL) [ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตน]
แหล่งข้อมูลที่น่าเชื่อถือ (Authoritative Source: AS)	แหล่งข้อมูลที่มีการให้ข้อมูลหรือจัดทำข้อมูลอย่างมีเหตุผล มีหลักเกณฑ์ หรือมีการอ้างอิงเพื่อให้ประชาชนหรือกลุ่มธุรกิจสามารถตรวจสอบหรือทราบข้อมูลต่าง ๆ ได้	ตัวอย่างแหล่งข้อมูลที่น่าเชื่อถือ เช่น ระบบตรวจสอบของหน่วยงานรัฐ ยกตัวอย่างในกรณีที่จะอ้างอิงตัวตนของคนไทยที่เป็นบุคคลธรรมดา ผู้ที่เป็น AS คือ กรมการปกครอง ซึ่งเป็นผู้จัดเก็บและตรวจสอบข้อมูลบัตรประจำตัวประชาชน

[3] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ขมธอ.18-2564 ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน โดยสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์

กระบวนการสมัครใช้และการพิสูจน์ตัวตน	กระบวนการใช้งานในการยืนยันตัวตน
1) บุคคลที่ประสงค์จะสมัครมี Digital ID มาแสดงตนกับ IdP ซึ่ง IdP จะพิสูจน์ตัวตนของบุคคลตามระดับความน่าเชื่อถือที่กำหนด (IAL) โดยอาจตรวจสอบหลักฐานแสดงตนและข้อมูลกับอัตลักษณ์กับ AS รวมถึงการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์นั้น	1) ผู้ใช้บริการขอเข้าใช้บริการหรือทำธุรกรรมกับ RP โดยใช้ Digital ID ที่มีระดับ IAL และ AAL ตามความต้องการของ RP
2) หากการพิสูจน์ตัวตนสำเร็จ IdP จะออกหรือลงทะเบียนสิ่งที่ใช้ยืนยันตัวตน และเชื่อมโยงอัตลักษณ์ของบุคคลกับสิ่งที่ใช้ยืนยันตัวตนนั้น โดย IdP มีหน้าที่เก็บรักษาข้อมูลเกี่ยวกับอัตลักษณ์ ข้อมูลการเชื่อมโยงอัตลักษณ์กับสิ่งที่ใช้ยืนยันตัวตน และสถานะของสิ่งที่ใช้ยืนยันตัวตน ตลอดอายุการใช้งานของสิ่งที่ใช้ยืนยันตัวตน	2) RP นำทาง (redirect) ให้ผู้ใช้บริการไปยืนยันตัวตน กับ IdP ว่าตนเองครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนตามเกณฑ์หรือระดับ AAL ที่กำหนด
3) บุคคลที่ผ่านการพิสูจน์ตัวตนแล้ว จะเปลี่ยนสถานะเป็น “ผู้ใช้บริการ” และมีหน้าที่ดูแลรักษาสิ่งที่ใช้ยืนยันตัวตนของตนเอง	3) IdP ตรวจสอบความถูกต้องและสถานะของสิ่งที่ใช้ยืนยันตัวตน แล้วส่งผลการยืนยันตัวตนให้กับ RP ซึ่ง RP สามารถใช้ข้อมูลจากผลการยืนยันตัวตนในการตัดสินใจที่จะให้บริการธุรกรรมหรือให้สิทธิในการเข้าใช้บริการ
	4) RP ทำการเชื่อมต่อกับผู้ใช้บริการเพื่อให้บริการธุรกรรมหรือให้เข้าใช้งานต่อไป



ภาพที่ 2 กระบวนการทำงานของ Digital ID

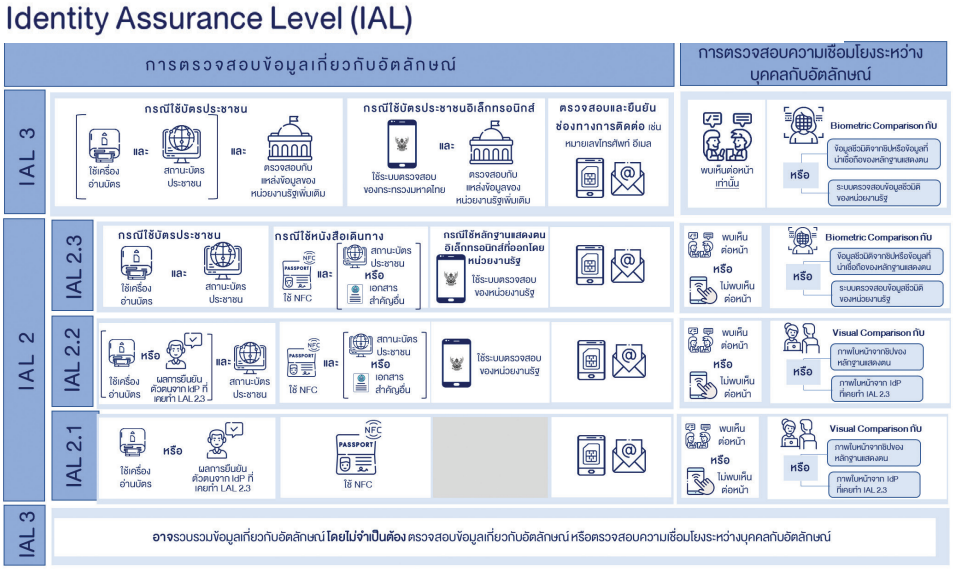
ที่มา: สพธอ. (2564ก) ดัดแปลงโดยผู้เขียน

สพธอ. มีการกำหนดระดับความน่าเชื่อถือของกระบวนการพิสูจน์และกระบวนการยืนยันตัวตน เพื่อเป็นการบริหารความเสี่ยงของการใช้ Digital ID แบ่งออกเป็น 1) ความเสี่ยงของการพิสูจน์ตัวตนผิดพลาด เช่น บุคคลที่มาพิสูจน์ตัวตนในขั้นตอนการสมัครใช้บริการแอบอ้างอัตลักษณ์ของบุคคลอื่นหรือใช้หลักฐานแสดงตัวตนปลอม และ 2) ความเสี่ยงของการยืนยันตัวตนผิดพลาด เช่น บุคคลที่แสดงสิ่งที่ใช้ยืนยันตัวตน (หรือ Digital ID) ไม่ใช่เจ้าของ Digital ID จริง ซึ่งผลกระทบที่อาจเกิดขึ้นจากความผิดพลาดของทั้งสองกระบวนการดังกล่าวคือการให้บริการธุรกรรมหรือให้สิทธิในการเข้าถึงการใช้งานระบบแก่บุคคลที่ไม่ถูกต้อง ดังนั้น ผู้ให้บริการจะต้องมีการประเมินความเสี่ยงของการพิสูจน์ตัวตนที่ผิดพลาดและการยืนยันตัวตนที่ผิดพลาดเพื่อให้สามารถกำหนดระดับความน่าเชื่อถือและเทคโนโลยีที่จะนำมาใช้ให้เหมาะสมกับการให้บริการ

ของตน โดย สพธอ. ได้กำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL)[4] และระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL)[5] โดยสรุปได้ดังนี้

ตารางที่ 2 การกำหนดระดับความน่าเชื่อถือของ Identity (Identity Assurance Level: IAL)

ระดับความน่าเชื่อถือของ Identity (Identity Assurance Level: IAL) คือ ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของบุคคล การกำหนด IAL ที่เหมาะสมจะช่วยลดโอกาสของการพิสูจน์ตัวตนที่ผิดพลาด โดย IAL แบ่งออกเป็น 3 ระดับหลัก ซึ่ง IAL1 คือความน่าเชื่อถือต่ำที่สุด และ IAL3 คือความน่าเชื่อถือสูงที่สุด	
ระดับ IAL1	อาจมีการรวบรวมข้อมูลอัตลักษณ์ ซึ่งเป็นข้อมูลที่ยืนยันด้วยตนเอง (self-asserted) อย่างไรก็ตาม IAL1 อาจมีการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์หรือการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์ด้วยวิธีการอื่น ๆ ตามความเสี่ยงของบริการธุรกรรม นอกเหนือจากวิธีการที่กำหนดไว้ในระดับ IAL2 และ IAL3 เช่น การตรวจสอบสำเนาหรือรูปถ่ายของหลักฐานแสดงตน (เช่น บัตรประจำตัวประชาชน) การตรวจสอบข้อมูลบนหน้าบัตรประจำตัวประชาชนและตรวจสอบสถานะของบัตรฯ การยืนยันช่องทางติดต่อ เช่น หมายเลขโทรศัพท์ อีเมล
ระดับ IAL2	กำหนดให้มีการขอหลักฐานการแสดงตน มีการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ว่าอัตลักษณ์ที่กล่าวอ้างเป็นข้อมูลของบุคคลที่มีอยู่จริง มีการตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับอัตลักษณ์นั้น การพิสูจน์ตัวตนที่ระดับ IAL2 สามารถทำได้ทั้งแบบพบเห็นต่อหน้า (face-to-face) หรือแบบไม่พบเห็นต่อหน้า (non face-to-face) เช่น การพิสูจน์ตัวตนผ่านเครื่องให้บริการ (kiosk) หรือแอปพลิเคชันของ IdP
ระดับ IAL3	เพิ่มระดับความเข้มงวดจากระดับ IAL2 โดยกำหนดให้มีการตรวจสอบกับแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานรัฐเพิ่มเติม และมีการตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับอัตลักษณ์ที่กล่าวอ้างด้วยการเปรียบเทียบข้อมูลชีวมิติ (biometric comparison) เพื่อป้องกันการปลอมตัวเป็นบุคคลอื่นและการลงทะเบียนซ้ำ ทั้งนี้ การพิสูจน์ตัวตนระดับ IAL3 สามารถทำได้แบบพบเห็นต่อหน้า (face-to-face) เท่านั้น



ภาพที่ 3 การกำหนดระดับความน่าเชื่อถือของ Identity (Identity Assurance Level: IAL)

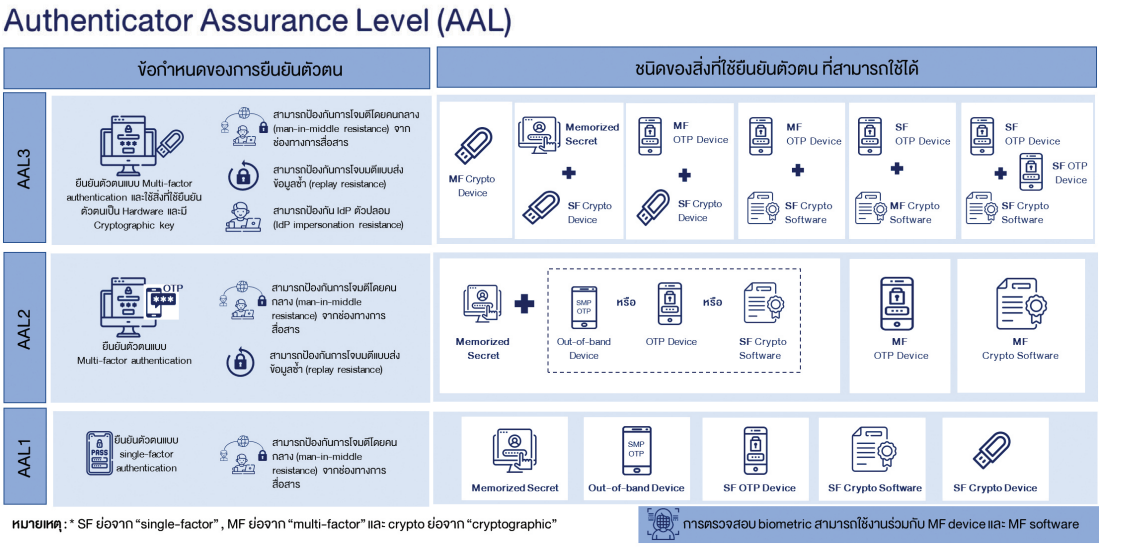
ที่มา: สพธอ. (2564v) ดัดแปลงโดยผู้เขียน

[4] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ขมธอ.18-2564 ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล–กรอบการทำงาน โดยสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ และข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ขมธอ.20-2564 ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล–ข้อกำหนดของการยืนยันตัวตน โดยสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์

[5] ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ขมธอ.18-2564 ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล–กรอบการทำงาน โดยสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ และข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ขมธอ.20-2564 ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล–ข้อกำหนดของการยืนยันตัวตน โดยสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์

ตารางที่ 3 การกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL)

ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL) คือ ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตน (Digital ID) การกำหนด AAL ที่เหมาะสมจะช่วยลดโอกาสการยืนยันตัวตนที่ผิดพลาด เช่น ผู้ที่ยืนยันตัวตนไม่ใช่เจ้าของ Digital ID หรือไม่ใช่บุคคลที่ลงทะเบียนและสมัครใช้ Digital ID กับ IdP โดย AAL แบ่งเป็น 3 ระดับหลัก ซึ่ง AAL1 คือความน่าเชื่อถือต่ำที่สุด และ AAL3 คือความน่าเชื่อถือสูงที่สุด	
ระดับ AAL1	ให้ความมั่นใจระดับหนึ่งว่าบุคคลที่กำลังเข้าใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ โดยระดับ AAL1 กำหนดให้ใช้วิธีการยืนยันตัวตนแบบปัจจัยเดียว (single-factor-authentication) เป็นอย่างน้อย
ระดับ AAL2	ให้ความมั่นใจระดับสูงว่าบุคคลที่กำลังเข้าใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ โดยระดับ AAL2 กำหนดให้ใช้การยืนยันตัวตนด้วยปัจจัย (authentication factor) ที่แตกต่างกัน 2 ปัจจัยเป็นอย่างน้อย
ระดับ AAL3	ให้ความมั่นใจระดับสูงมากว่าบุคคลที่กำลังเข้าใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ โดยระดับ AAL2 กำหนดให้ใช้การยืนยันตัวตนด้วยปัจจัย (authentication factor) ที่แตกต่างกัน 2 ปัจจัยเป็นอย่างน้อย และใช้สิ่งที่ใช้ยืนยันตัวตนที่มีคุณสมบัติเป็น hardware บรรจุกุญแจเข้ารหัส (cryptographic software) และสามารถป้องกัน IdP ตัวปลอม (IdP impersonation resistance)



ภาพที่ 4 การกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL)

ที่มา: สพธอ. (2564ค) ดัดแปลงโดยผู้เขียน

การเลือกระดับความน่าเชื่อถือของ IAL และ AAL ขึ้นอยู่กับผู้ให้บริการทำธุรกรรม กล่าวคือ หน่วยงานภาครัฐและเอกชนที่ให้บริการทำธุรกรรม จะเป็นผู้พิจารณาว่าต้องการระดับความเข้มงวดระดับใดที่เป็นการป้องกันความเสี่ยงที่อาจเกิดขึ้นได้ทั้งในขั้นตอนการพิสูจน์ตัวตน (เพื่อสมัครใช้ Digital ID) และการยืนยันตัวตน (ในขั้นตอนการให้บริการ) เพื่อป้องกันการแอบอ้างและความผิดพลาดและส่งผลกระทบต่อการให้บริการ องค์กร และความเชื่อมั่นของประชาชน ทั้งนี้ ในบางอุตสาหกรรมบริการ หน่วยงานกำกับดูแล เช่น ธนาคารแห่งประเทศไทย และสำนักงานป้องกันและปราบปรามการฟอกเงิน มีข้อกำหนดระดับความน่าเชื่อถือไว้ให้ผู้ให้บริการที่ตนกำกับดูแลปฏิบัติด้วย เช่น ในเรื่องการให้บริการเปิดบัญชีธนาคารนั้น

ธนาคารแห่งประเทศไทยกำหนดให้ใช้การพิสูจน์ตัวตนในระดับ IAL 2.3 และการยืนยันตัวตนในระดับ AAL 2 ซึ่งถือเป็นข้อกำหนดในระดับที่สูงเนื่องจากเป็นการให้บริการที่เกี่ยวข้องกับด้านการเงินการธนาคาร ในขณะที่บริการประเภทอื่น ๆ อาจใช้แค่ระดับมาตรฐานที่ IAL 2.1 หรือ IAL 1 เท่านั้น เพราะการให้บริการบางประเภทสามารถยอมรับระดับการพิสูจน์และยืนยันตัวตนที่ต่ำลงได้และไม่มีประเด็นความอ่อนไหวหรือสามารถยอมรับความเสี่ยงต่อการให้บริการของตนได้โดยมุ่งเน้นที่ความสะดวกแทน

4.4 หลักการและวิธีการทำงานทางปฏิบัติของ Mobile ID

จากหลักการขององค์ประกอบ โครงสร้าง และข้อกำหนดในเรื่องมาตรฐานต่าง ๆ ที่เกี่ยวข้องกับการให้บริการพิสูจน์และยืนยันตัวตนซึ่งเป็นส่วนประกอบของการให้บริการ Digital ID สามารถอธิบายหลักการและวิธีการทำงานทางปฏิบัติของ Mobile ID ซึ่งนำมาตรฐานของ สพธอ. มาปรับใช้งาน ดังนี้

4.4.1 การสมัครใช้งาน การพิสูจน์ตัวตน และออก Mobile ID

ผู้ให้บริการโทรศัพท์เคลื่อนที่ทำหน้าที่เป็นต้นน้ำของระบบการให้บริการทั้งหมด โดยทำหน้าที่ตั้งแต่การรับสมัครใช้ Mobile ID การพิสูจน์ตัวตนของผู้มาสมัครใช้ รวมถึงการออกและการบริหารจัดการ Mobile ID (IdP) เพราะผู้ให้บริการโทรศัพท์เคลื่อนที่ เป็นผู้ที่รู้จักตัวตนของผู้ใช้บริการของตนเองและมีการจัดเก็บข้อมูลของผู้ใช้บริการจากการลงทะเบียนซิม โดยมีขั้นตอนการทำงานและให้บริการดังนี้

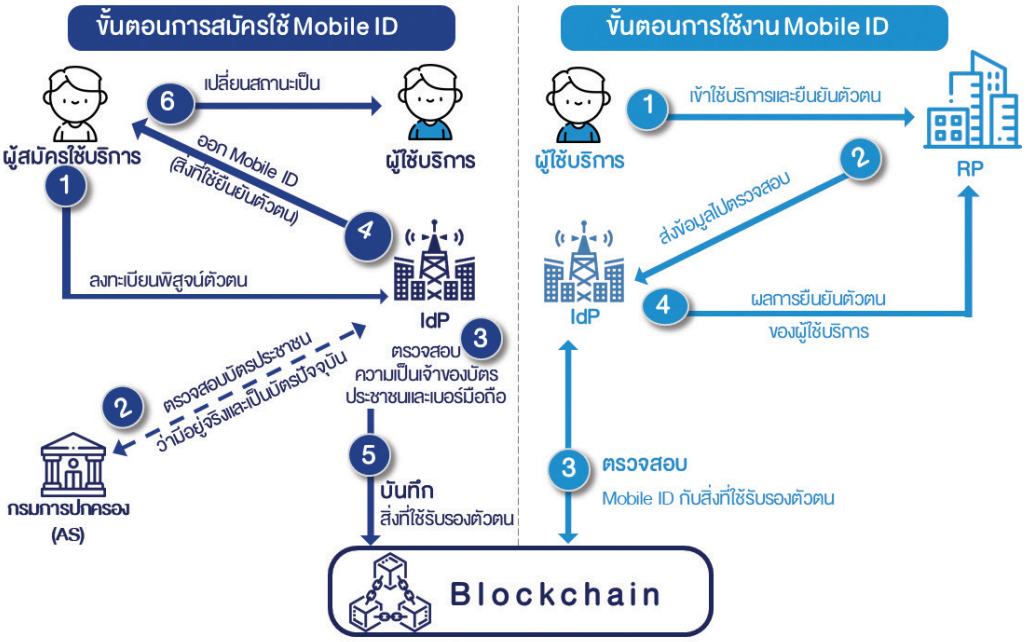
1) ผู้ใช้บริการโทรศัพท์เคลื่อนที่ที่ประสงค์จะสมัครใช้ Mobile ID ต้องไปสมัครและพิสูจน์ตัวตนที่ศูนย์ให้บริการของผู้ให้บริการโทรศัพท์เคลื่อนที่ (จุดให้บริการของ IdP) พร้อมแสดงบัตรประจำตัวประชาชนฉบับจริง โดยศูนย์ให้บริการจะตรวจสอบข้อมูลของบัตรประจำตัวประชาชนกับกรมการปกครอง ซึ่งเป็นหน่วยงานผู้ออกบัตร เพื่อตรวจสอบข้อมูลและสถานะของบัตรว่าเป็นบัตรปัจจุบันและมีสภาพทางกฎหมายอยู่หรือไม่ เช่น เป็นบัตรล่าสุดหรือไม่ หรือประชาชนคนนี้ยังมีชีวิตอยู่หรือไม่

2) ศูนย์ให้บริการจะทำการพิสูจน์ตัวตนว่าผู้สมัครเป็นเจ้าของบัตรประจำตัวประชาชนและเป็นเจ้าของหมายเลขโทรศัพท์หรือไม่ โดยใช้วิธีการตรวจสอบอัตลักษณ์บุคคลโดยนำบัตรประจำตัวประชาชนของผู้สมัครอ่านที่เครื่องอ่านบัตรสมาร์ตการ์ด (Smart Card Reader) ซึ่งเป็นเครื่องอ่านบัตรที่เราเคยเห็นที่ธนาคาร หรือร้านสะดวกซื้อ 7-11 ภาษาทั่วไปจะเรียกว่านำบัตรประจำตัวประชาชนมา “Dip chip” และถ่ายภาพใบหน้าของผู้สมัคร เพื่อให้ระบบเปรียบเทียบข้อมูลภาพถ่ายใบหน้าจาก 2 แหล่งคือ 1) ข้อมูลภาพถ่ายที่บรรจุในบัตรประจำตัวประชาชนอ่านจากเครื่องอ่านบัตรสมาร์ตการ์ด และ 2) ภาพถ่ายใบหน้าของผู้สมัครที่เจ้าหน้าที่ของศูนย์ให้บริการได้ถ่ายภาพไว้ ณ เวลาที่มาสมัคร หากตรวจสอบผ่านแสดงว่าผู้สมัครคนนั้นเป็นเจ้าของบัตรประจำตัว

ประชาชนตัวจริง ในขณะเดียวกันก็จะตรวจสอบความเป็นเจ้าของหมายเลขโทรศัพท์กับฐานข้อมูลการลงทะเบียนซิมของผู้ใช้บริการด้วย

3) เมื่อผ่านการตรวจสอบ ผู้ให้บริการโทรศัพท์เคลื่อนที่หรือ IdP จะสร้างและเก็บข้อมูลสิ่งที่ใช้ยืนยันตัวตนคือ Mobile ID และ “ผู้สมัคร” ก็จะเปลี่ยนสถานะเป็น “ผู้ใช้บริการ Mobile ID” และสามารถนำ Mobile ID ไปใช้งานได้

ขั้นตอนนี้ถือเป็นการขั้นตอนต้นน้ำที่มีความสำคัญมาก เพราะหากการพิสูจน์ตัวตนถูกต้องและมีมาตรฐาน การนำ Mobile ID ไปใช้งานก็จะมีความน่าเชื่อถือและปลอดภัย ซึ่งแสดงได้ดังภาพที่ 5



ภาพที่ 5 กระบวนและขั้นตอนการให้บริการ Mobile ID

4.4.2 การใช้งาน Mobile ID และการยืนยันตัวตนเพื่อใช้บริการ

เมื่อผู้ใช้บริการโทรศัพท์เคลื่อนที่ได้สมัครใช้ Mobile ID เรียบร้อยแล้ว สามารถนำไปใช้บริการกับผู้ให้บริการทั้งภาครัฐและเอกชนที่เข้าร่วมโครงการ (RP) โดย RP จะขอให้ผู้ให้บริการโทรศัพท์เคลื่อนที่หรือ IdP เป็นคนยืนยันตัวตนผู้ใช้บริการให้ (ดังภาพที่ 5) การให้บริการของ RP แบ่งออกเป็น 2 รูปแบบ คือ การให้บริการ ณ จุดให้บริการ (แบบพบเห็นต่อหน้า) เช่น ตามสถานที่ให้บริการต่าง ๆ หรือบนระบบออนไลน์ (แบบไม่พบเห็นต่อหน้า)

4.4.3 กรณีนำ Mobile ID ไปใช้งาน ณ จุดให้บริการ

1) ผู้ใช้บริการเข้าใช้แอปพลิเคชันของผู้ให้บริการโทรศัพท์เคลื่อนที่ที่เคยออก Mobile ID ให้ และเลือกใช้บริการ Mobile ID จากแอปพลิเคชัน จากนั้นใส่รหัส “Pin” ที่เคยตั้งไว้ และให้ความยินยอม (Consent) ในการเรียกใช้ QR Code เพื่อนำมาใช้ยืนยันตัวตน เมื่อดำเนินการสำเร็จก็จะมี QR Code ปรากฏขึ้น ซึ่งเป็น QR Code ส่วนบุคคลของผู้ใช้บริการผู้นั้น โดย QR Code บรรจุข้อมูล ได้แก่ เลขบัตรประจำตัวประชาชน 13 หลัก ชื่อ/นามสกุล เบอร์โทรศัพท์เคลื่อนที่ รหัสภาพถ่ายใบหน้าครึ่งหน้า (H1) (ถอดรหัสจากภาพถ่ายเมื่อตอนสมัครใช้ Mobile ID ที่ศูนย์ให้บริการ) Mobile ID serial no. และกำหนดระยะเวลาการใช้งาน QR Code (ดังภาพที่ 6 ขั้นตอน 1-3 และภาพที่ 8)

2) ในกรณีตัวอย่างจากภาพเป็นการเปิดบัญชีธนาคารที่สาขา โดยเจ้าหน้าที่ ณ สาขาธนาคารจะใช้เครื่องสแกน QR Code ที่ปรากฏบนโทรศัพท์ และถ่ายภาพใบหน้าของผู้ใช้บริการ ณ เวลานั้น เพื่อนำภาพใบหน้าจากทั้งสองแหล่งข้อมูลมาเปรียบเทียบด้วยระบบการตรวจสอบใบหน้า (จากรหัสภาพใบหน้าครึ่งหนึ่งที่บรรจุใน QR Code (H1) และรหัสใบหน้าอีกครึ่งหนึ่งที่ Mobile ID Platform เก็บไว้ตอนสมัครใช้ Mobile ID (H2) มาเข้ารหัสรวมกัน และทำการเปรียบเทียบกับภาพถ่ายใบหน้า ณ จุดให้บริการ) ซึ่งหากการเปรียบเทียบข้อมูลภาพรหัสใบหน้าตรงกันและผู้นั้นเป็นเจ้าของเบอร์โทรศัพท์ถูกต้อง ก็เป็นการยืนยันตัวตนว่าเป็นเจ้าของ Mobile ID และจึงให้บริการในขั้นตอนต่อไป ขั้นตอนนี้ ถือว่า IdP ตรวจสอบความถูกต้องของสถานะของสิ่งที่ใช้ยืนยันตัวตน คือ Mobile ID ให้กับผู้ให้บริการ RP (ดังภาพที่ 6 ขั้นตอน 4-6 และภาพที่ 8)

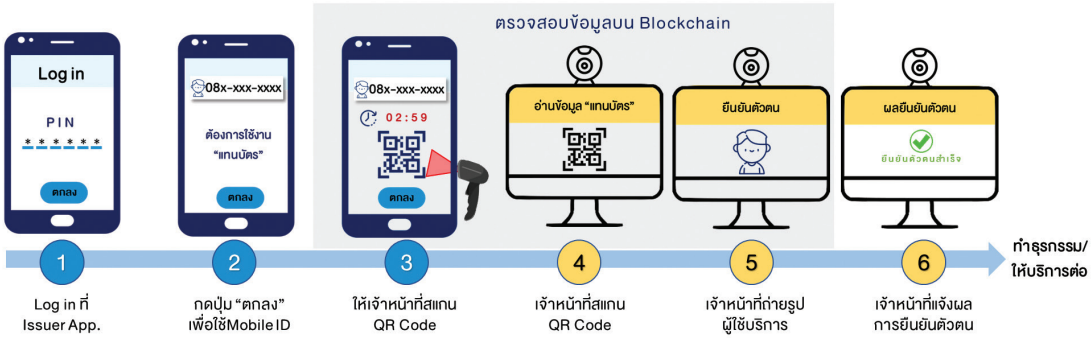
ทั้งนี้ ผู้ให้บริการ RP ก็สามารถนำข้อมูลใน QR Code ไปใช้งานต่อได้เช่นกัน ถือเป็นการใช้ Mobile ID แทนการใช้บัตรประจำตัวประชาชนและยืนยันตัวตนเพื่อเข้าใช้บริการหรือทำธุรกรรมต่าง ๆ โดย QR Code ที่มีการเรียกใช้แต่ละครั้งจะมีการเปลี่ยนแปลงทุกครั้งที่ถูกเรียกออกมาใช้งาน และมีการกำหนดระยะเวลาการใช้ QR Code ภายหลังจากถูกเรียกออกมาใช้งานด้วย สิ่งเหล่านี้คือการออกแบบเพิ่มเติมเพื่อให้การใช้ Mobile ID มีความปลอดภัย รักษาข้อมูลส่วนบุคคล และป้องกันการลักลอบแอบนำไปใช้งานด้วย

4.4.4 กรณีการนำ Mobile ID ไปใช้บริการออนไลน์ (ดังภาพที่ 7)

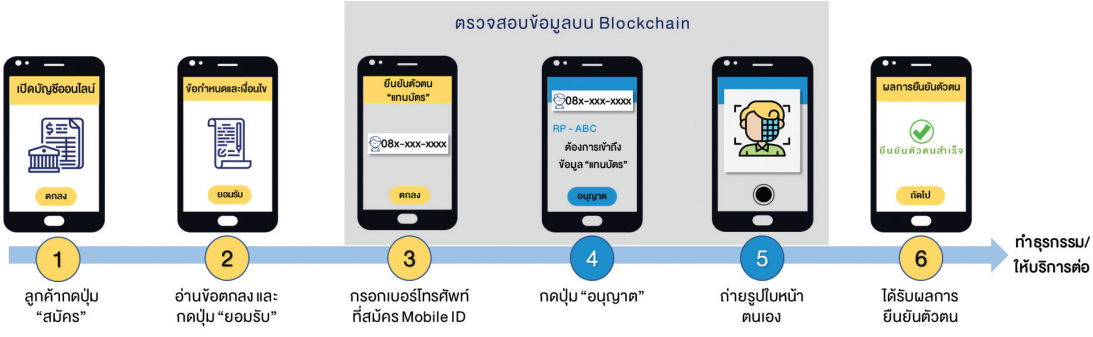
หลักการทำงานจะคล้ายกับรูปแบบแรก เพียงแต่การใช้งานผ่านระบบออนไลน์จะไม่มีการดึง QR Code ออกมาให้เห็น เพราะผู้ใช้บริการไม่ต้องพบเจอกับผู้ให้บริการ แต่มีการนำข้อมูลเหมือนกับที่บรรจุใน QR Code ไปใช้ตรวจสอบใน Mobile ID Platform โดยเมื่อ 1) ผู้ใช้บริการเข้าใช้แอปพลิเคชันหรือเว็บเบราว์เซอร์ (Web browser) ของผู้ให้บริการ RP ในกรณีตัวอย่างนี้เป็นการสมัครเปิดบัญชีธนาคาร

ทางช่องทางออนไลน์ 2) ผู้ใช้บริการยินยอมเงื่อนไขการใช้บริการ 3) ผู้ใช้บริการกรอกข้อมูลเลขหมายโทรศัพท์ที่มี Mobile ID 4) ผู้ให้บริการ RP จะมีการ Redirect ไปใช้แอปพลิเคชันของ IdP เพื่อให้ผู้ใช้บริการให้ความยินยอมในการให้ IdP ทำการยืนยันตัวตนให้ 5) ถ่ายภาพใบหน้าตนเอง (Selfie) เพื่อนำไปเปรียบเทียบกับข้อมูลในวิธีเดียวกับตัวอย่างของการใช้บริการที่จุดให้บริการข้างต้น

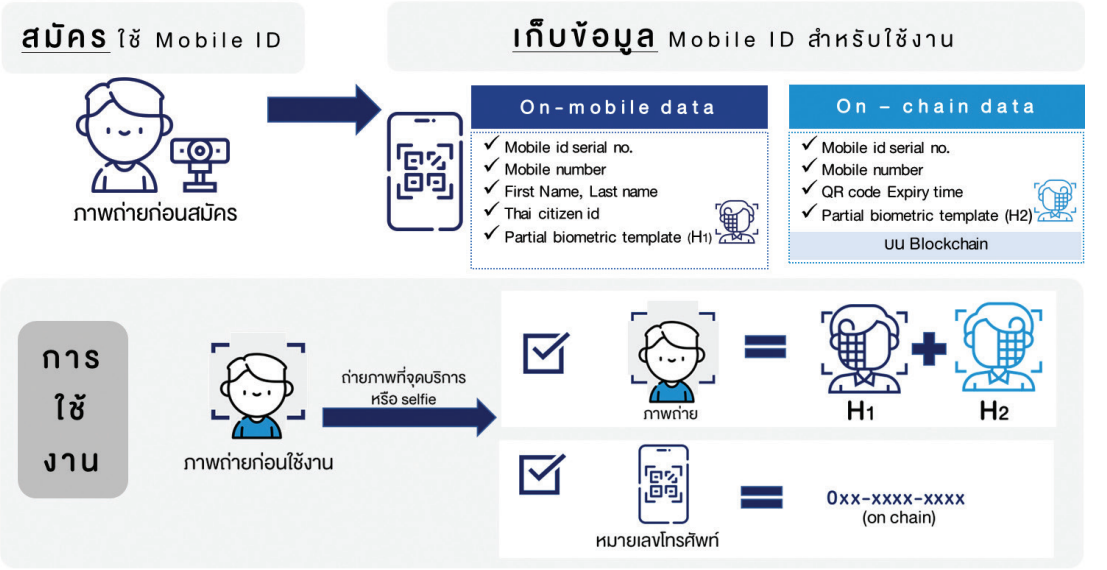
หากเปรียบเทียบการให้บริการ Mobile ID ในการดำเนินการพิสูจน์ตัวตน (ขั้นตอนการสมัครใช้ Mobile ID) และการยืนยันตัวตนในขั้นตอนการใช้บริการ (AAL) กับมาตรฐานความน่าเชื่อถือที่ สพธอ. กำหนดไว้นั้น จะเทียบเท่ากับ IAL 2.3 และ AAL 2 (ดูภาพที่ 3 และ 4 ประกอบ) ซึ่งเป็นมาตรฐานเทียบเท่ากับข้อกำหนดของธนาคารแห่งประเทศไทย และถือเป็นการเริ่มทดสอบทดลองในระดับที่มีความเชื่อมั่นขั้นสูง และส่งผลให้เกิดการยกระดับมาตรฐานการให้บริการของภาคโทรคมนาคมให้เทียบเท่ากับภาคธนาคาร



ภาพที่ 6 การใช้ Mobile ID เพื่อใช้บริการ ณ จุดให้บริการ (Face to Face)



ภาพที่ 7 การใช้ Mobile ID เพื่อใช้บริการบนช่องทางออนไลน์ (Non-Face to Face)



ภาพที่ 8 การจัดเก็บข้อมูลและการนำข้อมูลมาใช้โดยสังเขป

4.4.5 การบริหารจัดการของ Mobile ID Platform

กลไกหลักสำคัญที่ทำให้ทั้ง Ecosystem ของการให้บริการ Mobile ID ทำงานได้ คือ platform ซึ่งทำหน้าที่เชื่อมต่อการทำงานแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตน บันทึกข้อมูลที่จำเป็น เพื่อให้การใช้บริการและการให้บริการเป็นไปตามขั้นตอน มาตรฐานทางเทคนิค และระดับความปลอดภัยที่กำหนดไว้ ปัจจุบันในระยะทดสอบทดลอง สำนักงาน กสทช. เป็นผู้ลงทุน พัฒนา และบริหารจัดการ Mobile ID Platform โดยใช้เทคโนโลยีบล็อกเชน (Blockchain) รวมทั้งทำหน้าที่เป็นผู้กำกับดูแลการให้บริการและการใช้บริการบน platform ให้เป็นไปตามมาตรฐานและข้อกำหนดที่เกี่ยวข้องของ สพธอ.

4.5 การพัฒนาต่อยอด Mobile ID

จากการร่วมดำเนินงานกับทั้ง 14 หน่วยงาน ได้แก่ 1) ผู้ให้บริการโทรศัพท์เคลื่อนที่ที่ทำหน้าที่เป็น IdP 2) ผู้ให้บริการทำธุรกรรมภาครัฐและเอกชน (RP) และ 3) สำนักงาน กสทช. ที่ทำหน้าที่บริหารจัดการ platform เพื่อเชื่อมต่อการให้บริการของแต่ละส่วน ทุกฝ่ายได้ร่วมกันจัดทำเอกสารข้อกำหนดมาตรฐานการให้บริการ Mobile ID และผ่านการพิจารณาของ สพธอ. แล้ว โดยรวมถึงการกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) และการยืนยันตัวตน (AAL) ให้เหมาะสมกับกฎระเบียบและสอดคล้องกับรูปแบบการให้บริการประชาชน และพิจารณารูปแบบการให้บริการประชาชนที่นำมาทดสอบทดลอง (use case) ตามตารางที่ 4 โดยในปี พ.ศ. 2564 นี้จะมีการทดลองใช้ Mobile ID ในการเปิดบัญชีของธนาคารกรุงเทพ ทั้งกรณีการเปิดบัญชีที่สาขาของธนาคารและการเปิดบัญชีออนไลน์บนแอปพลิเคชันของธนาคาร และการใช้ Mobile ID แทนบัตรประจำตัวประชาชนสำหรับการจัดส่งพัสดุ ณ ที่ทำการบริษัท ไปรษณีย์ไทย จำกัด ก่อนเป็นลำดับแรก

ตารางที่ 4 ผู้ร่วมทดสอบทดลอง Mobile ID บทบาทที่เกี่ยวข้อง และการกำหนดทดสอบทดลอง

ผู้พิสูจน์และยืนยันตัวตน ผู้ออกและบริหารจัดการ Mobile ID Identity Provider (IdP)	ผู้ให้บริการกับประชาชน และผู้ใช้บริการยืนยันตัวตนจาก IdP Relying Party (RP)	รูปแบบบริการ
บริษัท แอดวานซ์ ไวร์เลส เน็ทเวอร์ค จำกัด บริษัท ทรู มูฟ เอช คอมมิวนิเคชั่น จำกัด บริษัท ดีแทค ไตรเน็ต จำกัด บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	ธนาคารกรุงเทพ	การเปิดบัญชีออนไลน์ และการเปิดบัญชีที่สาขา
	บริษัท ไปรษณีย์ไทย จำกัด	การส่งพัสดุ ณ ที่ทำการไปรษณีย์
	ตลาดหลักทรัพย์แห่งประเทศไทย	การให้บริการเปิดบัญชีลงทุน โดยเป็นตัวแทนให้กับบริษัทในตลาดหลักทรัพย์
	กรมสรรพากร	การยื่นชำระภาษีออนไลน์
	สำนักงานประกันสังคม	การลงทะเบียนเข้าสู่ระบบบริการขอใช้สิทธิประกันสังคม
	กรมการขนส่งทางบก	การสมัครใช้ใบอนุญาตขับขี่อิเล็กทรอนิกส์
	สถาบันคุ้มครองเงินฝาก	ใช้ Mobile ID ในการแสดงตนและยืนยันช่องทางการติดต่อ โดยผู้ที่ใช้ Mobile ID จะได้รับความสะดวกจากการคุ้มครองเงินฝากของสถาบันฯ มากขึ้น
	บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด	การขอตรวจสอบข้อมูลเครดิตสำหรับรายย่อย
	บริษัท ซีพี ออลล์ จำกัด (มหาชน)	การใช้บริการที่สาขาของร้านสะดวกซื้อ 7-11
กรมการปกครอง ทำหน้าที่เป็นแหล่งข้อมูลที่น่าเชื่อถือ (AS) ให้กับ IdP และ RP		
สำนักงาน กสทช. รับผิดชอบการลงทุน พัฒนา และบริหารจัดการ Mobile ID Platform รวมทั้งทำหน้าที่เป็นผู้กำกับดูแลการให้บริการและการใช้บริการบน platform ให้เป็นไปตามมาตรฐานที่ตกลงร่วมกันและสอดคล้องตามที่ สพธอ. กำหนด		

โครงการทดสอบทดลองการให้บริการ Mobile ID ที่ได้อธิบายมาข้างต้น เริ่มทดลองโดยเลือกใช้ระดับความน่าเชื่อถือในการพิสูจน์และยืนยันตัวตนอย่างจำกัดเพียงแค่ระดับ IAL 2.3 และ AAL 2 เท่านั้น เพื่อเป็นการทดลองให้เกิดความมั่นใจในขั้นแรก ทั้งด้านมาตรฐานการให้บริการ ด้านเทคนิค ด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และทดสอบรูปแบบการให้ประสบการณ์ที่ดีแก่ประชาชน อย่างไรก็ตาม Mobile ID จำเป็นต้องมีการพัฒนาต่อยอด ทั้งเรื่องรูปแบบการให้บริการ และการกำหนดบทบาทผู้รับผิดชอบในอนาคตที่จะเป็นแรงผลักดันและแรงเร่งให้เกิดการเติบโตในการใช้งาน Mobile ID อย่างแพร่หลายมากขึ้น เช่น การพัฒนาบริการ Mobile ID ให้ประชาชนสามารถมีและเข้าใช้โดยง่ายและทั่วถึง ดังนี้

1) เพิ่มความสะดวกให้ประชาชนสามารถสมัครใช้ Mobile ID ได้บนช่องทางออนไลน์ได้ โดยไม่จำเป็นต้องเดินทางไปสมัครใช้ที่ศูนย์บริการเท่านั้นดังตัวอย่างที่กล่าวมา เพื่อให้สอดรับกับพฤติกรรมของประชาชนในยุคปัจจุบันที่ชอบความสะดวกสบาย และมีความเข้าใจในการใช้เทคโนโลยีดิจิทัลมากขึ้นแล้ว อย่างไรก็ตาม ด้วยระดับความน่าเชื่อถือที่ สพธอ. กำหนดนั้น หากเป็นระดับที่สูงกว่า IAL1 ผู้สมัครใช้จะต้องนำบัตรประจำตัวประชาชนไปอ่านที่เครื่องอ่านบัตรสมาร์ตการ์ด ณ ศูนย์ให้บริการ กล่าวคือ แม้มีการสมัครใช้ Mobile ID ทางช่องทางออนไลน์แล้วก็ตาม แต่หากการทำธุรกรรมบางประเภทที่จำเป็นต้องอ้างอิงการพิสูจน์ตัวตนในระดับที่สูงกว่า IAL1 นั้น ผู้สมัครจะต้องไปหาสถานที่เพื่อ dip chip บัตรประจำตัวประชาชนของตนเพิ่มเติมอีก เช่น ไปที่ศูนย์ให้บริการของผู้ให้บริการโทรศัพท์เคลื่อนที่ หรือที่รับบริการ dip chip

เช่น ร้านสะดวกซื้อ 7-11 เพื่อให้การสมัครใช้ Mobile ID สมบูรณ์ตามข้อกำหนดของระดับความน่าเชื่อถือที่กำหนดไว้ ดังนั้น สพธอ. และหน่วยงานที่เกี่ยวข้อง เช่น กรมการปกครอง ควรต้องมีการพิจารณามาตรฐาน เทคโนโลยีอื่น หรือวิธีการอื่นที่ทันสมัย น่าเชื่อถือ ที่สามารถทดแทนการ dip chip บัตรประจำตัวประชาชนได้ ซึ่งเรื่องนี้ถือเป็นปัจจัยสำคัญประการหนึ่งที่จะผลักดันให้การใช้งาน Digital ID ของประเทศไทยมีการใช้งานเพิ่มมากขึ้น และเติบโตขึ้นได้อย่างมีนัยสำคัญ

2) สนับสนุนให้ผู้ประกอบการโทรศัพท์เคลื่อนที่สร้างกระบวนการในการสมัครใช้ Mobile ID เมื่อประชาชนเปิดใช้งานเลขหมายโทรศัพท์เคลื่อนที่ใหม่หรือซิมใหม่ในคราวเดียวกัน ซึ่งเป็นการสร้างความสะดวกในการเข้าใช้งาน Mobile ID โดยไม่ทำให้ประชาชนต้องเสียเวลามาทำการสมัครอีกครั้งหนึ่ง นอกจากนั้น หากมีการขยายการให้บริการกับนิติบุคคลและชาวต่างชาติด้วยก็จะทำให้การให้บริการ Mobile ID สามารถให้บริการครอบคลุมได้หลากหลายกลุ่มผู้ใช้บริการมากขึ้น โดยสำนักงาน กสทช. จะต้องมีการออกกฎเกณฑ์เพื่อให้การสนับสนุนผู้ให้บริการโทรศัพท์เคลื่อนที่ในกรณีเหล่านี้ด้วย

3) สนับสนุนให้ผู้ให้บริการโทรศัพท์เคลื่อนที่ที่เป็น IdP พัฒนารูปแบบการพิสูจน์ตัวตน และรูปแบบการยืนยันตัวตนให้มีระดับความน่าเชื่อถือที่หลากหลายที่สุด เพื่อเป็นทางเลือกให้กับผู้ให้บริการ RP และประชาชน โดยเพิ่มความสำคัญกับการให้บริการในระดับความน่าเชื่อถือที่ต่ำกว่าด้วย ซึ่งเป็นรูปแบบที่ทำให้การสมัครใช้ Mobile ID และการใช้งานนั้นสะดวกและง่ายขึ้น ไม่เป็นภาระเกินควรและสอดรับกับบริการทั่ว ๆ ไปในชีวิตประจำวันได้มากขึ้นและหลากหลายขึ้น เช่น การใช้ Mobile ID แทนการใช้บัตรประจำตัวประชาชนในการแลกบัตรเข้าอาคาร การสมัครสมาชิกบนบริการออนไลน์ต่าง ๆ หรือการใช้ Mobile ID แทนการใช้บัตรประชาชนในการเข้ารับการรักษาที่โรงพยาบาล เป็นต้น

4) พัฒนาให้ Mobile ID Platform สามารถให้บริการลงลายมือชื่ออิเล็กทรอนิกส์เพื่อทำธุรกรรมทางช่องทางออนไลน์ได้ ซึ่งถือเป็นการยกระดับและขยายรูปแบบการให้บริการ Mobile ID ให้สามารถรองรับการเข้าทำธุรกรรมที่จำเป็นต้องใช้ลายมือชื่อเพื่อให้มีผลทางกฎหมาย อันเป็นการขยายให้เกิดความต้องการของประชาชนที่หลากหลายขึ้น

5) เร่งกำหนดผู้บริหารจัดการ Mobile ID Platform ในอนาคตภายหลังจากการดำเนินงานในลักษณะการทดสอบทดลองเสร็จสมบูรณ์ นั่นหมายถึง Mobile ID Platform ควรจะแปรผันเป็นรูปแบบของธุรกิจการให้บริการและต้องขอรับใบอนุญาตจาก สพธอ. โดยหนึ่งในแนวทางที่เป็นไปได้ เช่น มีการจัดตั้งบริษัทใหม่ร่วมลงทุนระหว่างผู้ให้บริการโทรศัพท์เคลื่อนที่หรือเอกชนที่สนใจ เป็นต้น โดยบทบาทของสำนักงาน กสทช. ก็จะกลายเป็นผู้สนับสนุนบูรณาการงานสร้างสภาพแวดล้อมที่เอื้ออำนวยหรือแรงจูงใจในการให้บริการ และกำกับดูแลภายใต้กฎระเบียบที่กำหนด

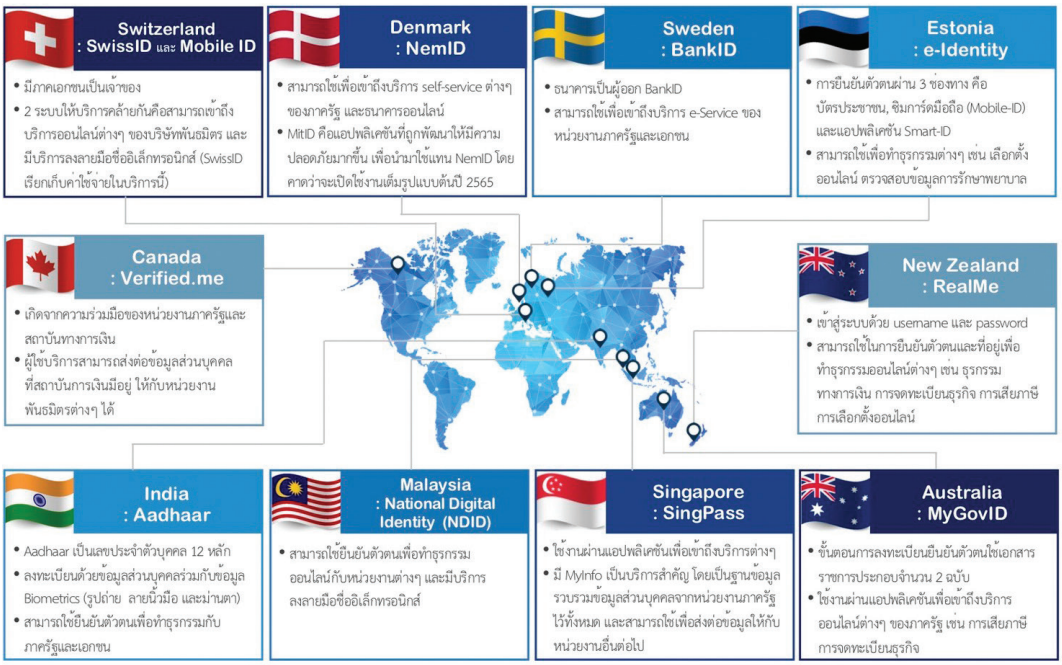
ตารางที่ 5 การเปรียบเทียบการให้บริการตามระดับความน่าเชื่อถือ IAL และ AAL ในช่วงทดสอบทดลองและอนาคต

IAL	Mobile ID ระยะทดสอบ	การพัฒนาระยะต่อไป	AAL	Mobile ID ระยะทดสอบ	การพัฒนาระยะต่อไป
IAL 3		√	AAL 3		√
IAL 2.3	√	√	AAL 2	√	√
IAL 2.2		√			
IAL 2.1		√			
IAL 1		√	AAL 1		√
ช่องทางสมัครใช้ Mobile ID	ศูนย์ให้บริการ	ศูนย์ให้บริการ และ Online			
เพิ่มการให้บริการที่หลากหลายที่สุด ให้ประชาชนเข้าใช้สะดวก และเพิ่มบริการการลงลายมือชื่ออิเล็กทรอนิกส์					

หมายเหตุ : แถบสีฟ้าคือสถานะปัจจุบันของการทดสอบทดลอง Mobile ID (ดูภาพที่ 3 และ 4 ประกอบ)

4.6 Digital ID Landscape ของประเทศไทย และ Mobile ID อยู่ตรงจุดใด

หลายประเทศทั่วโลกมีการพัฒนาการให้บริการและการใช้บริการ Digital ID อย่างแพร่หลาย และมีแนวโน้มเติบโตขึ้นอย่างต่อเนื่อง ตัวอย่างที่น่าสนใจของประเทศต่าง ๆ 10 ประเทศแสดงให้เห็นถึงการนำ Digital ID มาใช้ในเรื่องต่าง ๆ ดังนี้



ภาพที่ 9 ตัวอย่างการใช้งาน Digital ID ในต่างประเทศ

รูปแบบการให้บริการ Digital ID ที่ธนาคารโลกได้สรุปไว้[6] มีรูปแบบที่สำคัญ 3 รูปแบบ ซึ่งแต่ละประเทศก็มีทิศทางและใช้รูปแบบการให้บริการ Digital ID ที่แตกต่างกันขึ้นอยู่กับบริบทด้านนโยบายและสภาพแวดล้อมของประเทศนั้น ๆ

ตารางที่ 6 รูปแบบการให้บริการ Digital ID

รูปแบบ	ลักษณะ
แบบรวมศูนย์ (Centralised Operating Model)	หน่วยงานรัฐกำกับเต็มรูปแบบและเป็นเจ้าของข้อมูล Digital ID โดยรัฐทำหน้าที่เป็นผู้ออก Digital ID ให้กับประชาชน และผู้ให้บริการที่ต้องใช้บริการพิสูจน์และยืนยันตัวตนจะต้องเชื่อมต่อระบบกับหน่วยงานรัฐดังกล่าว
แบบกึ่งรวมศูนย์ (Semi-Centralised Operating Model)	หน่วยงานรัฐเป็นผู้กำกับดูแลและเป็นผู้อนุญาตให้มีการให้บริการ Digital ID ได้หลายราย โดยมีการออกกฎหมาย ระเบียบ มาตรฐาน และสร้างกระบวนการในการออกใบอนุญาตเพื่อการกำกับดูแลผู้ให้บริการและการให้บริการ
แบบกระจายศูนย์ (Distributed Operating Model)	ดำเนินการโดยอิสระ ผู้ให้บริการแต่ละรายอาจมีการเชื่อมโยงข้อมูลร่วมกัน โดยหน่วยงานรัฐอาจมีการออกมาตรฐานเพื่อให้ผู้ให้บริการใช้ร่วมกันแทนการกำกับดูแล

สำหรับกรณีประเทศไทย ได้มีการออก พ.ร.บ. ธุรกรรมอิเล็กทรอนิกส์ ฉบับที่ 4 เมื่อปี พ.ศ. 2562 และปัจจุบันมีการยกร่างพระราชกฤษฎีกาให้มีการกำหนดเรื่องการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (ปัจจุบันอยู่ระหว่างการพิจารณาของคณะกรรมการกฤษฎีกา) โดยส่งเสริมให้มีการประกอบธุรกิจในระบบใบอนุญาต เพื่อให้ประชาชนมีทางเลือกในการใช้บริการ ไม่ใช่เป็นลักษณะผูกขาดโดยรัฐหรือหน่วยงานใดหน่วยงานหนึ่งเป็นผู้ให้บริการ กล่าวคือ เปิดโอกาสให้ประเทศไทยมีการให้บริการ Digital ID ได้หลาย platform และเปิดโอกาสให้บริการที่เกี่ยวข้องกับ ecosystem ของ Digital ID มีผู้ประกอบหลายรายได้ตามกลไกตลาด เช่น บริการพิสูจน์ตัวตน (Identity Proofing Service) บริการยืนยันตัวตน (Authentication Service) บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital Identity Platform Service) ทั้งนี้ อยู่ภายใต้การอนุญาตและกำกับดูแลจาก สพธอ. เพื่อให้บริการมีความน่าเชื่อถือและปลอดภัย

ปัจจุบันการให้บริการ Digital ID Platform ของประเทศไทยที่มีการเริ่มให้บริการแล้วคือ National Digital ID (NDID) ซึ่งเป็นการร่วมลงทุนกันของบริษัทเอกชนโดยเฉพาะภาคธนาคาร มีการเริ่มให้บริการแล้วและเน้นบริการด้านการธนาคารในปัจจุบัน เช่น การเปิดบัญชีธนาคารทางออนไลน์ โดยแต่ละธนาคารมีการแลกเปลี่ยนข้อมูลและให้บริการพิสูจน์และยืนยันตัวตนระหว่างกัน หรือการใช้ NDID ในการยื่นเสียภาษีทางออนไลน์ของกรมสรรพากร เป็นต้น นอกจากนั้น มีการจัดทำระบบ D.DOPA ของกรมการปกครองเพื่อนำมาใช้พิสูจน์และยืนยันตัวตน และมี Mobile ID ที่อยู่ระหว่างการทดสอบทดลองในปัจจุบัน

[6] World Bank Group “Principle on Identification for Sustainable Development”

จากพื้นฐานด้านกฎหมายของประเทศไทยที่เน้นการให้อนุญาตกับผู้ประสงค์จะประกอบธุรกิจและส่งเสริมให้เกิดทางเลือกกับประชาชน และจากการขับเคลื่อนของหลายภาคส่วนที่เกิดขึ้นแล้วในปัจจุบัน แสดงให้เห็นว่าการให้บริการแบบรวมศูนย์ ที่ดำเนินการโดยรัฐเป็นผู้ออกและกำกับดูแลการใช้ Digital ID แต่เพียงผู้เดียวนั้นไม่สัมพันธ์กับบริบทของไทย โดยทิศทางของประเทศไทยควรจะมุ่งเน้นในรูปแบบกึ่งรวมศูนย์ที่มีการออกกฎหมายและกฎระเบียบที่ให้อำนาจหน่วยงานของรัฐในการกำกับดูแล รวมทั้งกำหนดมาตรฐานการให้บริการสำหรับผู้ให้บริการทั้งภาครัฐ (กำกับดูแลโดย สพร.) และเอกชน (กำกับดูแลโดย สพธอ.) นำไปใช้ ซึ่งรูปแบบกึ่งรวมศูนย์นี้มีข้อดีเนื่องจากเป็นรูปแบบที่เป็นไปตามกลไกตลาด และเปิดโอกาสให้มีผู้ให้บริการที่หลากหลาย มีการสร้างนวัตกรรมใหม่ ๆ และให้ประชาชนมีทางเลือกในการใช้บริการ ซึ่งจะสามารถขับเคลื่อนการใช้ Digital ID ของประเทศให้เติบโตได้อย่างรวดเร็ว ในขณะที่ผู้ให้บริการยังอยู่ภายใต้การกำกับดูแลที่เหมาะสมจากหน่วยงานรัฐ โดยรูปแบบกึ่งรวมศูนย์นี้เป็นรูปแบบที่สหราชอาณาจักรบริเตนใหญ่และไอร์แลนด์เหนือ เครือรัฐออสเตรเลีย ราชอาณาจักรสวีเดน และสาธารณรัฐฟินแลนด์ ใช้อยู่ในปัจจุบัน

การมี NDID และ D.DOPA เริ่มให้บริการในปัจจุบัน และในอนาคตที่จะมี Mobile ID ออกให้บริการ ไม่ใช่เรื่องของความซ้ำซ้อน แต่เป็นการเพิ่มรูปแบบการให้บริการ Digital ID ที่หลากหลายขึ้น และเป็นทางเลือกให้กับประชาชนได้เลือกใช้งานให้เหมาะสมกับสถานะเงื่อนไขและไลฟ์สไตล์ของตนเอง อย่างไรก็ตาม มีความเป็นไปได้ที่ Digital ID แต่ละ platform สามารถบูรณาการงานร่วมกันได้ (Interoperability) เช่น การเชื่อมต่อระบบระหว่าง Mobile ID และ NDID platform และอาจรวมถึง D.DOPA โดยแต่ละ platform สามารถนำจุดเด่นของตนเองมาสนับสนุนการให้บริการระหว่างกันได้ (complementary) เช่น ในการให้บริการพิสูจน์และยืนยันตัวตนของการเปิดบัญชีธนาคารของ NDID Platform อาจมีความต้องการตรวจสอบข้อมูลเลขหมายโทรศัพท์เคลื่อนที่ของผู้สมัครเปิดบัญชี ซึ่งธนาคารถือว่ามีความสำคัญในการใช้ติดต่อและอ้างอิงการใช้งาน โดย NDID Platform สามารถเชื่อมต่อกับ Mobile ID Platform เพื่อขอใช้บริการตรวจสอบและยืนยันความเป็นเจ้าของเลขหมายโทรศัพท์ของผู้สมัครเปิดบัญชีธนาคารจาก Mobile ID Platform ได้ ซึ่ง D.DOPA ก็อาจมีความต้องการเช่นเดียวกับ NDID เนื่องจาก Mobile ID platform เป็น platform เดียวที่สามารถตรวจสอบความเป็นเจ้าของเลขหมายโทรศัพท์เคลื่อนที่ได้ และในทางกลับกัน Mobile ID Platform ก็สามารถเชื่อมต่อกับ D.DOPA เพื่อตรวจสอบสถานะของบัตรประจำตัวประชาชนหรือเพื่อใช้ยืนยันตัวตนเพิ่มเติม ซึ่งทั้งหมดนี้คือประโยชน์ของการบูรณาการระบบร่วมกัน เพื่อลดการลงทุนที่ซ้ำซ้อนและประชาชนก็จะได้รับบริการที่ดีขึ้นด้วย โดยปัจจุบัน NDID ได้แจ้งความสนใจขอเชื่อมต่อกับระบบ Mobile ID Platform ด้วยแล้ว ซึ่งจะถือเป็นต้นแบบการทำงานร่วมกันครั้งสำคัญ

การดำเนินงานในลักษณะบูรณาการจำเป็นต้องมีการร่วมมือกันระหว่างหน่วยงานภาครัฐ โดยเฉพาะผู้กำกับดูแลแต่ละอุตสาหกรรมต้องเข้ามามีบทบาทในเรื่องนี้ กล่าวคือ สพธอ. เปรียบเสมือนผู้อนุญาตและกำกับดูแลการให้บริการ Digital ID ในภาพรวมของประเทศ และ สพร. ก็เปรียบเสมือนผู้กำกับดูแลและกำหนดกฎเกณฑ์การให้บริการของภาครัฐ ในขณะที่หน่วยงานกำกับดูแลแต่ละอุตสาหกรรม เช่น กสทช. ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เป็นต้น ที่มีกฎเกณฑ์ในการกำกับดูแลเฉพาะด้านของตนก็ต้องเข้ามามีบทบาทกำหนดรายละเอียดการให้บริการ Digital ID ให้เหมาะกับสภาพการให้บริการที่มีความแตกต่างกันและมีการกำกับดูแลเข้มข้นต่างกัน

ซึ่งตามโครงสร้างแล้วมีความเป็นไปได้ที่ สพธอ. จะกำหนดทิศทางของกฎหมายที่มอบอำนาจให้หน่วยงานกำกับดูแลแต่ละภาคอุตสาหกรรมมีบทบาทในการกำหนดกฎเกณฑ์เฉพาะ และเป็นผู้กำกับดูแลและตรวจสอบการทำงานของผู้ให้บริการ Digital ID ในภาคบริการของตน ดังนั้น การกำหนดนโยบายที่ชัดเจน การบูรณาการงานและการกำหนดกฎเกณฑ์ระหว่างหน่วยงานร่วมกัน ซึ่งรวมถึงการกำหนดมาตรฐานร่วมกันระหว่าง platform เพื่อการแลกเปลี่ยนและเชื่อมโยงข้อมูลกัน จึงเป็นเรื่องที่จำเป็นและน่าท้าทาย และถือเป็นการสร้างรากฐานที่เข้มแข็งของการพัฒนาการให้บริการ Digital ID ของประเทศไทยในอนาคต

5. บทสรุปและข้อเสนอแนะ

บทบาทที่เปลี่ยนแปลง สร้างโอกาสที่ดีขึ้นให้สังคม

การดำเนินงานเรื่อง Mobile ID นี้ ถือเป็นตัวอย่างหนึ่งที่เป็นบทบาทการทำงานแนวใหม่ของสำนักงาน กสทช. ที่นอกเหนือจากดำเนินการด้านการกำกับดูแลและบริหารงานตามที่กฎหมายกำหนด โดยเป็นบทบาทของผู้ริเริ่ม (initiative) ผู้สนับสนุน (enabler) และผู้แทนของอุตสาหกรรมโทรคมนาคม (representative) ในการทำงานร่วมกับภาคส่วนอื่น ๆ เพื่อให้อุตสาหกรรมโทรคมนาคมนำศักยภาพและจุดเด่นของตนไปสนับสนุนภาคอุตสาหกรรมต่าง ๆ รวมทั้งสามารถสร้างมูลค่าเพิ่ม ก่อให้เกิดโอกาสทางธุรกิจและโอกาสที่ประชาชนจะได้รับบริการในโลกยุคใหม่ที่ดีขึ้น โดยรูปแบบการทำงานนี้เป็นโมเดลที่สำนักงาน กสทช. ควรนำไปใช้ในการพัฒนางานด้านอื่น ๆ ตามที่สำนักงาน กสทช. จะเห็นโอกาสหรือสร้างโอกาสให้เกิดขึ้น

ในปลายปีนี้ประชาชนจะได้เริ่มทดลองใช้บริการ Mobile ID โดยหากในอนาคตมีการพัฒนาให้สามารถรองรับบริการที่หลากหลายขึ้นทั้งสำหรับประชาชนผู้ใช้งานและสำหรับหน่วยงานภาครัฐและเอกชน รวมทั้งมีการพัฒนาให้ประชาชนสามารถเข้าถึงการสมัครใช้บริการได้สะดวก และมีการกำหนดโมเดลทางธุรกิจที่ชัดเจน ก็จะเป็นการสร้างโอกาสให้ Mobile ID เติบโต เป็นที่รู้จัก และเป็นที่นิยมของประชาชนในวงกว้าง นอกจากนั้น Mobile ID จะเป็นเครื่องมือและสะพานเชื่อมที่จะทำให้การพิสูจน์และยืนยันตัวตนของบริการบนโลกออนไลน์หรือบริการ over-the-top (OTT) ต่าง ๆ มีคุณภาพและน่าเชื่อถือขึ้น และเป็นเครื่องมือหนึ่งที่จะส่งเสริมการใช้ Mobile ID และการให้บริการธุรกรรมอิเล็กทรอนิกส์ของประเทศไทยให้เติบโต และในที่สุดจะเป็นสิ่งที่ประชาชนนิยมใช้และเชื่อมั่น จนกลายเป็นส่วนหนึ่งสำหรับการใช้ชีวิตในโลกดิจิทัลที่สะดวกและปลอดภัย

“Mobile ID แทนบัตร แทนตัวคุณ”

บรรณานุกรม

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2564ก). *ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ขมธอ.18-2564 ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – กรอบการทำงาน* https://standard.etda.or.th/wp-content/uploads/2021/10/20210930-ER-V2-DID-1-Framework-V08-16F.pdf

_____. (2564ข). *ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ขมธอ.19-2561 ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – ข้อกำหนดของการพิสูจน์ตัวตน* https://standard.etda.or.th/wp-content/uploads/2021/10/20210930-ER-V2-DID-2-IdentityProofing-V08-16F.pdf

_____. (2564ค). *ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ขมธอ.20-2564 ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล - ข้อกำหนดของการยืนยันตัวตน* https://standard.etda.or.th/wp-content/uploads/2021/10/20210930-ER-V2-DID-3-Authentication-V08-16F.pdf

McKinsey Global Institute. (2019). *Digital identification: A key to inclusive growth.* https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20gro wth/MGI-Digital-identification-Report.ashx

World Bank Group. (2021). *Principles on Identification for Sustainable Development : Toward the Digital Age (English).* https://documents.worldbank.org/en/publication/documents-reports/documentdetail/213581486378184357/principles-on-identification-for-sustainable-development-toward-the-digital-age