

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล

โดยที่เป็นการสมควรปรับปรุงมาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล สำหรับใช้อ้างอิงและเลือกใช้งานดิจิทัลไอดี เพื่อให้การนำมาตรฐานมาใช้ในการพิสูจน์และยืนยันตัวตนทางดิจิทัล เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพยิ่งขึ้น

อาศัยอำนาจตามความในมาตรา ๓๗ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๓) พ.ศ. ๒๕๖๒ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ให้ยกเลิกประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล ลงวันที่ ๑๕ กันยายน พ.ศ. ๒๕๖๖

ข้อ ๒ ให้นำมาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล ดังต่อไปนี้ โดยมีรายละเอียดปรากฏตามแนบท้ายประกาศ มาใช้ในการพิสูจน์และยืนยันตัวตนทางดิจิทัล

(๑) มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล เล่ม ๑: กรอบการทำงาน เลขที่ มธอ. ๑๑ เล่ม ๑-๒๕๖๖

(๒) มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล เล่ม ๒: ข้อกำหนดของการพิสูจน์ตัวตน เลขที่ มธอ. ๑๑ เล่ม ๒-๒๕๖๙

(๓) มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล เล่ม ๓: ข้อกำหนดของการยืนยันตัวตน เลขที่ มธอ. ๑๑ เล่ม ๓-๒๕๖๖

ข้อ ๓ ให้มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล เล่ม ๒: ข้อกำหนดของการพิสูจน์ตัวตน เลขที่ มธอ. ๑๑ เล่ม ๒-๒๕๖๖ ข้อ ๔.๒ ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ ในระดับ IAL ๒.๓ (๑) แห่งประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล ลงวันที่ ๑๕ กันยายน พ.ศ. ๒๕๖๖ ยังคงมีผลใช้บังคับได้ต่อไปเป็นเวลาหนึ่งปี นับแต่วันที่ประกาศนี้ใช้บังคับ เฉพาะกรณีที่ได้ทำการพิสูจน์ตัวตนแบบพบเห็นต่อหน้าซึ่งตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตรประจำตัวประชาชนและตรวจสอบสถานะของบัตรประจำตัวประชาชนโดยใช้หมายเลขหลังบัตรประจำตัวประชาชน (laser code)

ประกาศ ณ วันที่ ๓๐ ตุลาคม พ.ศ. ๒๕๖๙

(นางวิลาวรรณ มังคละธนะกุล)
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

ELECTRONIC TRANSACTION STANDARD

มธอ. 11 เล่ม 1-2566

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 1: กรอบการทำงาน

DIGITAL IDENTITY –
PART 1: FRAMEWORK

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.030

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 1: กรอบการทำงาน

มธอ. 11 เล่ม 1-2566

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 20-22
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ประธานกรรมการ

นางอรรชกา สีบุญเรือง

รองประธานกรรมการ

นายวิศิษฏ์ วิศิษฏ์สรอรรถ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

กรรมการผู้ทรงคุณวุฒิ

นางสาวสิริธิดา พนมวัน ณ อยุธยา
นายศีลวัต สันติวิสัฏฐ์
นายปณิธิ ชุณหสวัสดิกุล
นายอนุชิต อนุชิตานุกูล
นายกนิษฐ์ สารสิน
นางสาวช่อผกา วิริยานนท์
นายเฉลิมรัฐ นาควิเชียร
นายยรรยง เต็งอำนวย

กรรมการและเลขานุการ

นายชัยชนะ มิตรพันธ์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คณะอนุกรรมการกลั่นกรองการกำหนดหลักเกณฑ์ในการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ประธานอนุกรรมการ

นางสาวอัจฉรินทร์ พัฒนพันธ์ชัย

อนุกรรมการ

นายอนันต์ กนกศิลป์	สำนักงานปลัดกระทรวงสาธารณสุข
นางรุ่งนิภา อมาตยคง	
นายสัญชัย เตชนิมิตวัช	กรมการปกครอง
นายอภิวัฒน์ อินขัด	กรมการกงสุล
นางศิริพร ชำนาญชาติ	กรมพัฒนาธุรกิจการค้า
นางสาวรัญศิกานต์ งามบุษบงโสภา	
นางสาวสิริธิดา พนมวัน ณ อยุธยา	ธนาคารแห่งประเทศไทย
นางสาววิจิตรเลขา มารมย์	
นางสาวสายชล แซ่ลี้	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
นางสาวจิตสถา ศรีประเสริฐสุข	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และ
นางสาวอรวรี เจริญพร	กิจการโทรคมนาคมแห่งชาติ
นายสมเกียรติ วัฒนาประสบสุข	สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
นายณัฐวุฒิ ทิพย์กนก	
นายณรงค์เดช วัชระภาสร	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
นายกิตตินันท์ ศรีมงคล	
นายวิบูลย์ ภัทรพิบูล	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
นายอภิสิทธิ์ สุขสาคร	
นายพีรธร วิมลโลหการ	สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นางสาวอุรัชฎา เกตุพรหม	
นายจำรัส สว่างสมุทร	คณะกรรมการร่วมภาคเอกชน ๓ สถาบัน
นายวิเชียร เปรมชัยสวัสดิ์	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นายณัฐวุฒิ อมรวิวัฒน์	

เลขานุการ

นางสาวพลอย เจริญสม	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คณะอนุกรรมการมาตรฐานและการกำกับดูแล

ประธานอนุกรรมการ

นายยรรยง เต็งอำนวย

อนุกรรมการ

รองศาสตราจารย์ปริทรรศน์ พันธุบรรยงก์	
นายปริญญา หอมเอนก	
นางสาวภรณี หรูวรรธนะ	
นายรอม หิรัญพฤกษ์	
นางสาวสุธีรา ศรีไพบูลย์	
นายอนุชิต อนุชิตานุกูล	
นางสาวสุดจิตร ลาภเลิศสุข	กรมบัญชีกลาง
นางสาวภิญญู กำเนิดหล่ม	กรมสรรพากร
นางสาวรัญศิกานต์ งามบุษบงโสภา	กรมพัฒนาธุรกิจการค้า
นายก่อเกียรติ แก้วกิ่ง	กรมการปกครอง
นางศิริพร ช่างการ	สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม
นายสมเกียรติ วัฒนาประสบสุข	สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
นายกำพล ศรธนะรัตน์	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
นายเนติพงษ์ ตลับนาค	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
นายสินชัย ต่อวัฒนกิจกุล	สำนักงานหลักประกันสุขภาพแห่งชาติ
นางบุษกร ธีระปัญญาชัย	ธนาคารแห่งประเทศไทย
นายภิญโญ ตรีเพชราภรณ์	
นายเอธ แย้มประทุม	
นายสุพจน์ เธียรวุฒิ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายวิบูลย์ ภัทรพิบูล	
นายวีระ วีระกุล	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นางสาวธิดารัช ธนภรรคภวิน	

อนุกรรมการและเลขานุการ

นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ช่วยเลขานุการ

นายสิริณัฐ ตั้งธรรมจิต	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คำนำ

ด้วยการเข้าทำธุรกรรมต่าง ๆ จำเป็นต้องมีกระบวนการพิสูจน์และยืนยันตัวตนผู้ที่ประสงค์จะเข้าทำธุรกรรมก่อนเพื่อให้มั่นใจได้ว่าผู้ที่ประสงค์จะเข้าทำธุรกรรมเป็นบุคคลนั้นจริง ประกอบกับในปัจจุบันมีการทำธุรกรรมและการให้บริการในรูปแบบดิจิทัลเพิ่มมากขึ้น ผู้ให้บริการจึงเริ่มมีการพัฒนากระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัลเพื่ออำนวยความสะดวกในการเข้าใช้บริการต่าง ๆ ในขณะเดียวกันกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ได้มีการแก้ไขปรับปรุงเพื่อรองรับให้บุคคลสามารถพิสูจน์และยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ ซึ่งกลไกดังกล่าวสามารถลดภาระต่อผู้ใช้บริการในการแสดงตน การส่งเอกสารหรือหลักฐานประกอบการพิสูจน์และยืนยันตัวตน รวมถึงช่วยลดขั้นตอนที่ต้องทำกระบวนการเดิมซ้ำ ๆ เพื่อพิสูจน์ตัวตนก่อนเข้าทำธุรกรรม

อย่างไรก็ตาม กระบวนการพิสูจน์และยืนยันตัวตนในปัจจุบันยังมีความหลากหลายและมีข้อกำหนดแตกต่างกันไปตามเงื่อนไขและความจำเป็นของผู้ให้บริการหรือหน่วยงานแต่ละแห่งซึ่งในบางกรณีอาจเกิดความไม่สอดคล้องหรือไม่สามารถนำมาใช้งานร่วมกันได้ ดังนั้น จึงได้มีการพัฒนามาตรฐานเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัลโดยการดำเนินการที่ผ่านมาสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชนได้ร่วมกันจัดทำมาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัล ได้แก่ ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ (ETDA Recommendation) ซึ่งมีการพัฒนาและปรับปรุงมาอย่างต่อเนื่อง ดังนี้

- เวอร์ชัน 1.0: เลขที่ ขมธอ. 18-2561, 19-2561 และ 20-2561
- เวอร์ชัน 2.0: เลขที่ ขมธอ. 18-2564, 19-2564 และ 20-2564
- เวอร์ชัน 3.0: เลขที่ ขมธอ. 18-2566, 19-2566 และ 20-2566

ในการนี้ เพื่อให้เกิดความสอดคล้องและเสริมสร้างความน่าเชื่อถือและยอมรับในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล และเพื่อให้ผู้ให้บริการและหน่วยงานต่าง ๆ สามารถใช้อ้างอิงและเลือกใช้งานดิจิทัลไอดีร่วมกันได้บนมาตรฐานและระดับความน่าเชื่อถือที่มีความสอดคล้องกัน คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงเห็นควรให้มีการยกระดับมาตรฐานดังกล่าว โดยนำข้อเสนอแนะมาตรฐานฯ เลขที่ ขมธอ. 18-2566, 19-2566 และ 20-2566 มาปรับปรุงเป็นชุดมาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล (เลขที่ มธอ. 11) ซึ่งประกอบด้วย

- เล่ม 1 กรอบการทำงาน (Part 1: Framework)
- เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน (Part 2: Identity Proofing Requirements)
- เล่ม 3 ข้อกำหนดของการยืนยันตัวตน (Part 3: Authentication Requirements)

สำหรับการพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 1 กรอบการทำงาน ฉบับนี้ เป็นเอกสารอธิบายคำศัพท์ กระบวนการ การประเมินความเสี่ยง และการกำหนดระดับความน่าเชื่อถือที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อให้ผู้ที่เกี่ยวข้องกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความเข้าใจตรงกัน

สารบัญ

หน้า

1. ขอบข่าย **1**

2. บทนิยาม **1**

3. การพิสูจน์และยืนยันตัวตนทางดิจิทัล **2**

3.1 ภาพรวม 2

3.2 ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้อง 3

3.3 สิ่งที่ใช้ยืนยันตัวตน 4

3.4 ผลการยืนยันตัวตน 6

3.5 ดิจิทัลไอดีแบบ Federated Identity 6

4. การกำหนดระดับความน่าเชื่อถือ **7**

4.1 ภาพรวม 7

4.2 ระดับความน่าเชื่อถือ 7

4.3 การประเมินความเสี่ยงเพื่อกำหนดระดับความน่าเชื่อถือ 7

4.4 ตัวอย่างการกำหนดระดับความน่าเชื่อถือ 9

ภาคผนวก ก. อักษรย่อ **12**

บรรณานุกรม **13**

สารบัญรูป

หน้า

รูปที่ 1 ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้องในการพิสูจน์ตัวตนและยืนยันตัวตน 3

สารบัญตาราง

หน้า

ตารางที่ 1 เกณฑ์การประเมินระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด 8

ตารางที่ 2 ระดับผลกระทบที่เป็นไปได้และระดับความน่าเชื่อถือที่ต้องการ 9

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 1: กรอบการทำงาน

1. ขอบข่าย

มาตรฐานฉบับนี้อธิบายคำศัพท์ กระบวนการ การประเมินความเสี่ยง และการกำหนดระดับความน่าเชื่อถือที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อให้ผู้ที่เกี่ยวข้องกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความเข้าใจตรงกัน

2. บทนิยาม

ความหมายของคำที่ใช้ในมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 การพิสูจน์และยืนยันตัวตน หมายถึง กระบวนการพิสูจน์และยืนยันความถูกต้องของตัวบุคคล [1]

2.2 อัตลักษณ์ (identity) หมายถึง ลักษณะเฉพาะของบุคคลซึ่งสามารถบ่งบอกหรือจำแนกได้โดยคุณลักษณะหรือชุดของคุณลักษณะที่เกี่ยวข้องกับตัวบุคคลนั้น [2]

หมายเหตุ 1: ตัวอย่างของคุณลักษณะที่เกี่ยวข้องกับบุคคลธรรมดา เช่น เลขประจำตัว ชื่อบุคคล ที่อยู่ วันเดือนปีเกิด อีเมล หมายเลขโทรศัพท์เคลื่อนที่ ภาพใบหน้า หรือข้อมูลระบุอุปกรณ์ที่บุคคลใช้งาน

หมายเหตุ 2: ตัวอย่างของคุณลักษณะที่เกี่ยวข้องกับนิติบุคคล เช่น เลขทะเบียนนิติบุคคล ชื่อนิติบุคคล ที่ตั้งสำนักงานใหญ่ หรือชื่อกรรมการของนิติบุคคล

2.3 หลักฐานแสดงตน (identity evidence) หมายถึง เอกสารทางกายภาพหรือข้อมูลอิเล็กทรอนิกส์ ซึ่งสามารถใช้เป็นหลักฐานในการพิสูจน์ตัวตน

2.4 การพิสูจน์ตัวตน (identity proofing) หมายถึง กระบวนการรวบรวมและตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคล และการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์นั้น [2]

2.5 สิ่งที่ใช้ยืนยันตัวตน (authenticator) หมายถึง สิ่งที่ใช้เชื่อมโยงอัตลักษณ์กับบุคคล ซึ่งบุคคลนั้นครอบครองและควบคุมเพื่อใช้ในการยืนยันตัวตน เช่น รหัสผ่าน ข้อมูลชีวภาพ [2]

2.6 การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน หมายถึง กระบวนการเชื่อมโยงอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้ยืนยันตัวตน และการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนนั้น [2]

2.7 การยืนยันตัวตน (authentication) หมายถึง กระบวนการยืนยันอัตลักษณ์ของบุคคลด้วยการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้น [2]

2.8 ผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) หมายถึง หน่วยงานที่ให้บริการแก่บุคคลภายนอกเกี่ยวกับการพิสูจน์ตัวตน การออกและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน หรือการยืนยันตัวตน ทั้งนี้ ผู้พิสูจน์และยืนยันตัวตนอาจมอบหมายงานบางส่วนให้ผู้ให้บริการภายนอก (outsourcing) หรือตัวแทนของผู้พิสูจน์และยืนยันตัวตน (agent) โดยผู้พิสูจน์และยืนยันตัวตนรับผิดชอบเสมือนเป็นผู้ดำเนินการเอง

2.9 ผู้อาศัยการยืนยันตัวตน (relying party: RP) หมายถึง บุคคลหรือหน่วยงานที่พึ่งพาอาศัยผลการยืนยันตัวตนจาก IdP หรือสิ่งที่ใช้ยืนยันตัวตนที่ผู้ใช้บริการมีอยู่ก่อนแล้ว ในการตัดสินใจที่จะให้บริการธุรกรรมหรือให้สิทธิในการเข้าใช้งานระบบ

2.10 แหล่งข้อมูลที่น่าเชื่อถือ (authoritative source: AS) หมายถึง แหล่งข้อมูลที่มีการให้ข้อมูลหรือจัดทำข้อมูลอย่างมีเหตุผล มีหลักเกณฑ์ หรือมีการอ้างอิง เพื่อให้ประชาชนหรือกลุ่มธุรกิจสามารถตรวจสอบหรือทราบข้อมูลต่าง ๆ ได้

หมายเหตุ: ตัวอย่างของแหล่งข้อมูลที่น่าเชื่อถือ เช่น ระบบตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยหน่วยงานของรัฐ

2.11 ผู้ใช้บริการ (subscriber) หมายถึง บุคคลที่ผ่านการพิสูจน์ตัวตนและได้รับสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ในการยืนยันตัวตน

2.12 ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL) หมายถึง ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของบุคคล

2.13 ระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL) หมายถึง ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตน

3. การพิสูจน์และยืนยันตัวตนทางดิจิทัล

3.1 ภาพรวม

อัตลักษณ์ (identity) คือ ลักษณะเฉพาะของบุคคลซึ่งสามารถบ่งบอกหรือจำแนกได้โดยคุณลักษณะหรือชุดของคุณลักษณะที่เกี่ยวข้องกับตัวบุคคลนั้น ในขณะที่ดิจิทัลไอดี (digital identity) จะเป็นอัตลักษณ์ที่บันทึกในรูปแบบอิเล็กทรอนิกส์ ซึ่งบุคคลสามารถนำดิจิทัลไอดีไปใช้ในการทำธุรกรรมทางอิเล็กทรอนิกส์ ทั้งนี้ดิจิทัลไอดีของแต่ละบุคคลจะต้องมีความเฉพาะเจาะจงในบริบทของบริการธุรกรรมหนึ่ง ๆ แต่อาจไม่จำเป็นต้องมีความเฉพาะเจาะจงในทุกบริบท อย่างไรก็ตาม บริการธุรกรรมบางประเภทอาจไม่มีความเข้มงวดในการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการ เช่น การให้บริการอีเมลหรือสื่อสังคมออนไลน์ ขณะที่บริการธุรกรรมประเภทที่มีความเสี่ยงสูง เช่น การให้บริการทางการเงิน ผู้ให้บริการจะต้องทราบข้อมูลเกี่ยวกับอัตลักษณ์ที่แท้จริงของผู้ใช้บริการสำหรับใช้เป็นดิจิทัลไอดีในการทำธุรกรรมทางอิเล็กทรอนิกส์

การพิสูจน์ตัวตน (identity proofing) เป็นกระบวนการที่ผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) รวบรวมและตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคล และตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์นั้น โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าอัตลักษณ์ที่กล่าวอ้างเป็นอัตลักษณ์ของบุคคลนั้นจริง (เช่น บุคคลที่กล่าวอ้างว่าตนเองชื่อ “สมชาย” คือ “สมชาย” ตัวจริง ไม่ใช่บุคคลอื่นปลอมตัวมา) ทั้งนี้มาตรฐานฉบับนี้กำหนดความเข้มงวดของกระบวนการพิสูจน์ตัวตนเป็นระดับที่เรียกว่า “ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)”

บุคคลที่ผ่านการพิสูจน์ตัวตนเรียบร้อยแล้วจะเปลี่ยนสถานะเป็น “ผู้ใช้บริการ (subscriber)” และได้รับสิ่งที่ใช้ยืนยันตัวตน (authenticator) เพื่อใช้ในการยืนยันอัตลักษณ์ของบุคคล เมื่อผู้ใช้บริการต้องการเข้าใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์กับผู้อาศัยการยืนยันตัวตน (relying party: RP) ซึ่งเป็นผู้ให้บริการที่ต้องการทราบข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการก่อนตัดสินใจที่จะให้บริการธุรกรรมดังกล่าว

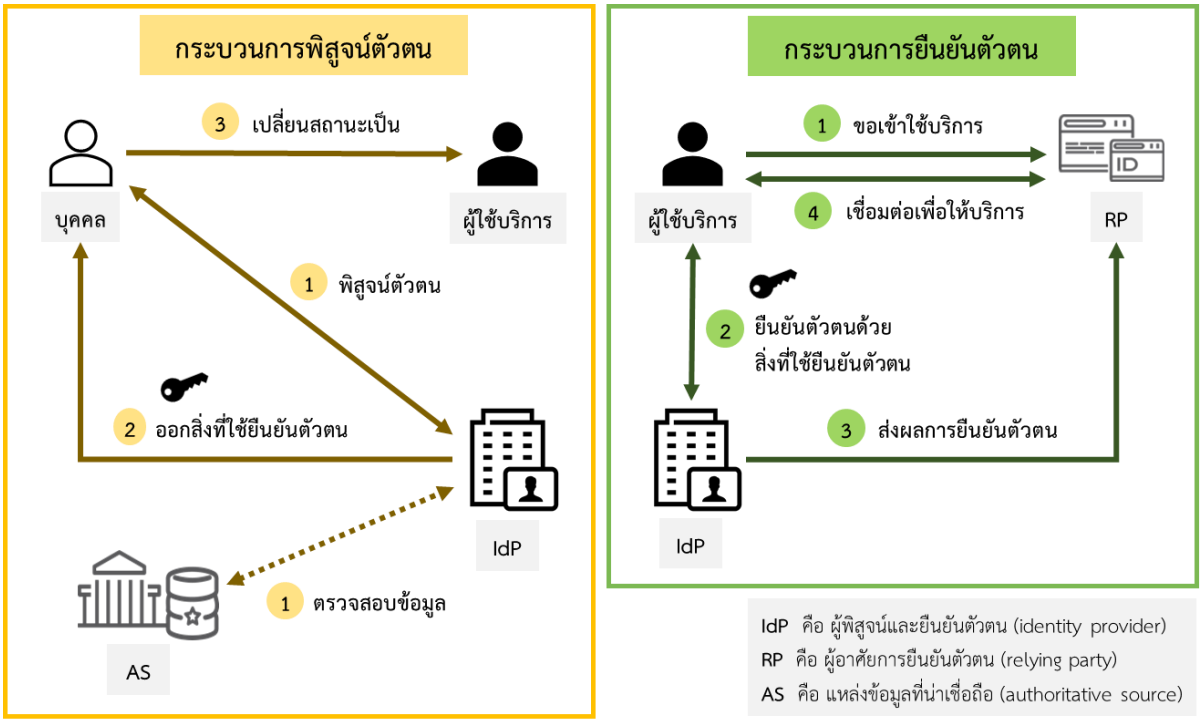
RP จะขอให้ IdP ที่ผู้ใช้บริการเคยผ่านการพิสูจน์ตัวตนและได้รับสิ่งที่ใช้ยืนยันตัวตนมาก่อน ช่วยดำเนินการยืนยันตัวตนของผู้ใช้บริการ

การยืนยันตัวตน (authentication) เป็นกระบวนการยืนยันอัตลักษณ์ของบุคคลด้วยการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนของบุคคลนั้น โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าบุคคลที่กำลังเข้าใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนนั้นจริง (เช่น บุคคลที่กำลังเข้าใช้บริการ คือ “สมชาย” ตัวจริง ที่กรอกรหัสผ่านถูกต้อง) ทั้งนี้ มาตรฐานฉบับนี้กำหนดความเข้มงวดของกระบวนการยืนยันตัวตนเป็นระดับที่เรียกว่า “ระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL)”

เมื่อผู้ใช้บริการสามารถยืนยันตัวตนกับ IdP ได้ว่าตนเองครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนจริงตามเกณฑ์วิธี (protocol) ที่กำหนด IdP จะส่งผลการยืนยันตัวตน (assertion) ให้กับ RP เพื่อใช้ในการตัดสินใจที่จะให้บริการธุรกรรมหรือให้สิทธิในการเข้าใช้งานระบบ โดยผลการยืนยันตัวตนอาจประกอบด้วยผลการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน และข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการ เช่น เลขประจำตัว ชื่อบุคคล วันเดือนปีเกิด ที่อยู่อีเมล หมายเลขโทรศัพท์เคลื่อนที่ หรือคุณลักษณะอื่น ๆ ที่รวบรวมไว้ในกระบวนการพิสูจน์ตัวตน ซึ่งขึ้นอยู่กับนโยบายของ IdP ความต้องการของ RP และความยินยอมในการเปิดเผยข้อมูลของเจ้าของข้อมูล

3.2 ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้อง

ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้องในการพิสูจน์ตัวตนและยืนยันตัวตน แสดงเป็นแผนภาพตามรูปที่ 1 โดยด้านซ้ายของรูปจะเป็นกระบวนการพิสูจน์ตัวตน และด้านขวาของรูปจะเป็นกระบวนการยืนยันตัวตน



รูปที่ 1 ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้องในการพิสูจน์ตัวตนและยืนยันตัวตน

กระบวนการพิสูจน์ตัวตนมีขั้นตอนทั่วไป ดังนี้

(1) บุคคลที่ประสงค์จะมีดิจิทัลไอดีสำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์มาแสดงตนกับ IdP ซึ่ง IdP จะพิสูจน์ตัวตนของบุคคลตามระดับ IAL ที่กำหนด โดยอาจมีการตรวจสอบหลักฐานแสดงตนและข้อมูลเกี่ยวกับอัตลักษณ์กับ AS รวมถึงการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์นั้น

(2) หากการพิสูจน์ตัวตนสำเร็จ IdP จะออกหรือลงทะเบียนสิ่งที่ใช้ยืนยันตัวตน และเชื่อมโยงอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้ยืนยันตัวตนนั้น โดย IdP มีหน้าที่เก็บรักษาข้อมูลเกี่ยวกับอัตลักษณ์ ข้อมูลการเชื่อมโยงอัตลักษณ์กับสิ่งที่ใช้ยืนยันตัวตน และสถานะของสิ่งที่ใช้ยืนยันตัวตน ตลอดอายุการใช้งานของสิ่งที่ใช้ยืนยันตัวตน

(3) บุคคลที่ผ่านการพิสูจน์ตัวตนแล้วจะเปลี่ยนสถานะเป็นผู้ใช้บริการ และมีหน้าที่ดูแลรักษาสิ่งที่ใช้ยืนยันตัวตนของตนเอง

กระบวนการยืนยันตัวตนซึ่งเกิดขึ้นเมื่อผู้ใช้บริการต้องการเข้าใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์กับ RP มีขั้นตอนทั่วไป ดังนี้

(1) ผู้ใช้บริการขอเข้าใช้บริการหรือทำธุรกรรมกับ RP โดยใช้ดิจิทัลไอดีที่มีระดับ IAL และ AAL สอดคล้องตามความต้องการของ RP

(2) RP นำทาง (redirect) หรือแนะนำให้ผู้ใช้บริการไปยืนยันตัวตนกับ IdP ที่ผู้ใช้บริการเคยผ่านการพิสูจน์ตัวตนมาก่อน และให้ผู้ใช้บริการยืนยันตัวตนกับ IdP ว่าตนเองครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนตามเกณฑ์วิธีหรือระดับ AAL ที่กำหนด

(3) IdP ตรวจสอบความถูกต้องและสถานะของสิ่งที่ใช้ยืนยันตัวตน แล้วส่งผลการยืนยันตัวตนให้กับ RP ซึ่ง RP สามารถใช้ข้อมูลจากผลการยืนยันตัวตนในการตัดสินใจที่จะให้บริการธุรกรรมหรือให้สิทธิในการเข้าใช้งานระบบกับผู้ใช้บริการ

(4) RP ทำการเชื่อมต่อกับผู้ใช้บริการเพื่อให้บริการธุรกรรมหรือให้เข้าใช้งานระบบ

ทั้งนี้ RP และ IdP อาจเป็นหน่วยงานเดียวกัน (กรณีที่ IdP ออกสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ภายในกิจการของหน่วยงาน) หรือเป็นคนละหน่วยงานกัน (กรณีที่ IdP ออกสิ่งที่ใช้ยืนยันตัวตนเพื่อให้บริการแก่บุคคลภายนอก)

3.3 สิ่งที่ใช้ยืนยันตัวตน

สิ่งที่ใช้ยืนยันตัวตน (authenticator) คือ สิ่งที่ใช้เชื่อมโยงอัตลักษณ์กับบุคคล ซึ่งบุคคลนั้นครอบครองและควบคุม เพื่อใช้ในการยืนยันตัวตนกับ IdP ทั้งนี้ สิ่งที่ใช้ยืนยันตัวตนทุกอันจะมีปัจจัยของการยืนยันตัวตน (authentication factor) อย่างน้อยหนึ่งปัจจัย โดยปัจจัยของการยืนยันตัวตนแบ่งออกเป็น 3 ประเภท ดังนี้

(1) สิ่งที่คุณรู้ (something you know) คือ ข้อมูลที่ผู้ใช้บริการเท่านั้นที่ทราบ เช่น รหัสผ่าน (password) และเลขรหัสส่วนตัว (PIN)

(2) สิ่งที่คุณมี (something you have) คือ สิ่งของที่ผู้ใช้บริการเท่านั้นครอบครอง เช่น กุญแจเข้ารหัส (cryptographic key) อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device) และอุปกรณ์ OTP (OTP device)

(3) สิ่งที่คุณเป็น (something you are) คือ ข้อมูลชีวมิติ (biometric data) ของผู้ใช้บริการ เช่น ภาพใบหน้า และลายนิ้วมือ

สิ่งที่ใช้ยืนยันตัวตนอาจประกอบด้วยปัจจัยของการยืนยันตัวตนเพียงหนึ่งปัจจัย (การยืนยันตัวตนแบบปัจจัยเดียว: single-factor authentication) หรือประกอบด้วยปัจจัยของการยืนยันตัวตนมากกว่าหนึ่งปัจจัย (การยืนยันตัวตนแบบหลายปัจจัย: multi-factor authentication) โดยความเข้มงวดของระบบการยืนยันตัวตนจะขึ้นอยู่กับจำนวนปัจจัยของการยืนยันตัวตนและความสามารถในการป้องกันการโจมตีของระบบการยืนยันตัวตน อย่างไรก็ตาม IdP หรือ RP อาจใช้ข้อมูลประกอบอื่น ๆ เช่น ข้อมูลระบุตำแหน่ง หรือข้อมูลระบุอุปกรณ์ที่บุคคลใช้งาน เพื่อเพิ่มความมั่นคงปลอดภัยของระบบการยืนยันตัวตน แต่ข้อมูลเหล่านี้จะไม่ถือเป็นปัจจัยของการยืนยันตัวตน

ในการยืนยันตัวตนแบบไม่พบเห็นต่อหน้า ผู้ใช้บริการต้องแสดงให้เห็นว่าตนเองครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนที่ได้ลงทะเบียนไว้กับ IdP เพื่อยืนยันว่าตนเองเป็นเจ้าของอัตลักษณ์ที่กล่าวอ้างจริง เนื่องจากสิ่งที่ใช้ยืนยันตัวตนจะมีข้อมูลลับ (secret) ที่เฉพาะผู้ใช้บริการตัวจริงเท่านั้นสามารถนำมาใช้ยืนยันตัวตนได้ ทั้งนี้ ข้อมูลลับในสิ่งที่ใช้ยืนยันตัวตนสามารถเป็นคู่กุญแจอสมมาตร (asymmetric keys) หรือข้อมูลลับใช้ร่วมกัน (shared secret)

กรณีที่ข้อมูลลับเป็นคู่กุญแจอสมมาตรซึ่งประกอบด้วยกุญแจส่วนตัว (private key) และกุญแจสาธารณะ (public key) ที่สัมพันธ์กัน ผู้ใช้บริการจะใช้กุญแจส่วนตัวในสิ่งที่ใช้ยืนยันตัวตนเพื่อยืนยันตัวตน ส่วน IdP จะใช้กุญแจสาธารณะที่สัมพันธ์กับกุญแจส่วนตัวเพื่อยืนยันว่าผู้ใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนที่มีกุญแจส่วนตัวนั้น (โดยทั่วไปกุญแจสาธารณะจะอยู่ในรูปแบบใบรับรองกุญแจสาธารณะ (public key certificate))

กรณีที่ข้อมูลลับเป็นข้อมูลลับใช้ร่วมกัน ข้อมูลลับในสิ่งที่ใช้ยืนยันตัวตนอาจเป็นกุญแจสมมาตร (symmetric keys) หรือรหัสลับจดจำ (memorized secret) โดยข้อแตกต่าง คือ กุญแจสมมาตรถูกเลือกจากระบบสุ่มและเก็บไว้ในฮาร์ดแวร์หรือซอฟต์แวร์ที่อยู่ภายใต้การควบคุมของผู้ใช้บริการ ขณะที่รหัสลับจดจำเป็นข้อมูลลับที่ให้ผู้ใช้บริการจดจำ ซึ่งโดยทั่วไป กุญแจเข้ารหัสไม่ว่าจะเป็นกุญแจสมมาตรหรือกุญแจส่วนตัวมักจะมีความยาวของอักขระมากกว่ารหัสลับจดจำ จึงทำให้มีความซับซ้อนที่ยากแก่การคาดเดาโดยผู้ไม่ประสงค์ดี

หมายเหตุ: หลักฐานแสดงตน เช่น บัตรประจำตัวประชาชนหรือใบขับขี่ (ปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี) ซึ่งไม่มีข้อมูลลับในรูปแบบอิเล็กทรอนิกส์ แม้ว่าจะสามารถนำมาใช้ยืนยันตัวตนแบบพบเห็นต่อหน้ากับบุคคล (เช่น เจ้าหน้าที่รักษาความปลอดภัย) แต่ไม่สามารถนำมาใช้ยืนยันตัวตนแบบไม่พบเห็นต่อหน้าได้ เนื่องจากระบบคอมพิวเตอร์ไม่มีข้อมูลให้ตรวจสอบหรือยืนยันตัวตนของผู้ใช้บริการได้

การยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) ซึ่งมีการใช้ปัจจัยของการยืนยันตัวตนมากกว่าหนึ่งปัจจัย สามารถทำได้ 2 วิธี ดังนี้

(1) การใช้ปัจจัยของการยืนยันตัวตนมากกว่าหนึ่งปัจจัยเพื่อยืนยันตัวตนกับ IdP โดยตรง เช่น ผู้ใช้บริการต้องกรอกทั้งรหัสผ่าน (สิ่งที่คุณรู้) และข้อมูลลับที่ส่งมายังโทรศัพท์เคลื่อนที่ของผู้ใช้บริการทาง SMS (สิ่งที่คุณมี) เพื่อยืนยันตัวตนกับ IdP

(2) การใช้ปัจจัยของการยืนยันตัวตนบางปัจจัยเพื่อปกป้องข้อมูลลับก่อนที่จะใช้ยืนยันตัวตนกับ IdP เช่น การใช้ลายนิ้วมือ (สิ่งที่คุณเป็น) เพื่อปกป้องกุญแจส่วนตัว (สิ่งที่คุณมี) ในโทรศัพท์เคลื่อนที่

โดยผู้ใช้บริการต้องสแกนลายนิ้วมือเพื่อทำให้ซอฟต์แวร์เข้ารหัสลับ (cryptographic software) ในโทรศัพท์เคลื่อนที่สามารถเรียกใช้กุญแจส่วนตัวเพื่อยืนยันตัวตนกับ IdP

3.4 ผลการยืนยันตัวตน

หากการยืนยันตัวตนสำเร็จ IdP จะส่งผลการยืนยันตัวตน (assertion) ให้กับ RP โดยผลการยืนยันตัวตนอาจประกอบด้วยผลการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน และข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการ ทั้งนี้ IdP อาจส่งผลการยืนยันตัวตนไปยัง RP โดยตรงผ่านช่องทางที่มั่นคงปลอดภัยเพื่อรักษาความครบถ้วน (integrity) ของผลการยืนยันตัวตน หรืออาจส่งผลการยืนยันตัวตนไปยัง RP ผ่านผู้ใช้บริการ ซึ่ง IdP ต้องจัดให้มีวิธีการรักษาความครบถ้วนของผลการยืนยันตัวตนเพื่อไม่ให้มีการเปลี่ยนแปลงแก้ไขในภายหลัง

RP จะเชื่อถือผลการยืนยันตัวตนหรือไม่ขึ้นอยู่กับแหล่งที่มา เวลาที่สร้าง และสถานะปัจจุบันของผลการยืนยันตัวตน รวมถึงนโยบายของ RP และ IdP ที่เกี่ยวข้องกับความน่าเชื่อถือของการพิสูจน์และยืนยันตัวตน นอกจากนี้ RP ต้องตรวจสอบแหล่งที่มา (IdP) และการรักษาความครบถ้วนของผลการยืนยันตัวตน เพื่อให้มั่นใจว่าผลการยืนยันตัวตนไม่ถูกเปลี่ยนแปลงแก้ไขระหว่างการส่งมาจาก IdP ก่อนที่ RP จะนำผลการยืนยันตัวตนไปใช้ในการตัดสินใจต่อไป

หากมีการส่งผลการยืนยันตัวตนผ่านช่องทางที่เป็นเครือข่ายสาธารณะ (public network) IdP ต้องมีวิธีการรักษาความลับ (confidentiality) ของข้อมูลส่วนบุคคลของผู้ใช้บริการที่อยู่ในผลการยืนยันตัวตน เพื่อให้มั่นใจว่าเฉพาะ RP ที่กำหนดเท่านั้นสามารถเข้าถึงข้อมูลได้

3.5 ดิจิทัลไอดีแบบ Federated Identity

ดิจิทัลไอดีแบบ federated identity เป็นรูปแบบการใช้งานดิจิทัลไอดีที่ผู้ใช้บริการสามารถให้ IdP ส่งผลการยืนยันตัวตนเกี่ยวกับผู้ใช้บริการให้กับ RP ที่เป็นคนละระบบหรือคนละหน่วยงานได้ รวมถึง RP อาจพึ่งพาอาศัยผลการยืนยันตัวตนจาก IdP มากกว่าหนึ่งรายก็ได้ โดย IdP และ RP สามารถเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกันผ่านเครือข่ายหรือระบบกลางที่ช่วยอำนวยความสะดวกด้านเทคนิคในการเชื่อมต่อและตั้งค่าระบบของ IdP RP และผู้ที่เกี่ยวข้องอื่น ๆ

การใช้งานดิจิทัลไอดีแบบ federated identity มีประโยชน์หลายอย่าง เช่น

(1) เพิ่มความสะดวกให้กับผู้ใช้บริการ โดยผู้ใช้บริการสามารถพิสูจน์ตัวตนกับ IdP รายใดรายหนึ่ง และนำสิ่งที่ใช้ยืนยันตัวตนที่ได้รับจาก IdP นั้นมาใช้ยืนยันตัวตนเพื่อเข้าใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์กับ RP หลายรายได้

(2) ลดค่าใช้จ่ายให้กับ RP ในการพัฒนาโครงสร้างพื้นฐานทางเทคโนโลยี (เช่น การจัดการบัญชีผู้ใช้งานและสิ่งที่ใช้ยืนยันตัวตน) และลดภาระของผู้ใช้บริการในการครอบครองหรือเก็บรักษาสิ่งที่ใช้ยืนยันตัวตนที่แตกต่างกันของ RP แต่ละราย เนื่องจาก RP ในกลุ่มเดียวกันสามารถอาศัยสิ่งที่ใช้ยืนยันตัวตนหรือข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการร่วมกันได้

(3) ทำให้หน่วยงานสามารถมุ่งเน้นการดำเนินงานไปที่ภารกิจหลักของหน่วยงานโดยตรง แทนที่การดำเนินงานด้านการพิสูจน์และยืนยันตัวตน

4. การกำหนดระดับความน่าเชื่อถือ

4.1 ภาพรวม

ความเสี่ยงที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนตามมาตรฐานฉบับนี้ แบ่งออกเป็น 2 ด้าน คือ ความเสี่ยงของการพิสูจน์ตัวตนที่ผิดพลาด (เช่น บุคคลที่มาพิสูจน์ตัวตนแอบอ้างอัตลักษณ์ของบุคคลอื่นหรือใช้หลักฐานแสดงตนปลอม) และความเสี่ยงของการยืนยันตัวตนที่ผิดพลาด (เช่น บุคคลที่แสดงสิ่งที่ใช้ยืนยันตัวตนไม่ใช่เจ้าของสิ่งที่ใช้ยืนยันตัวตนจริง) โดยผลกระทบที่อาจเกิดขึ้นจากความผิดพลาดของการพิสูจน์และยืนยันตัวตน คือ การให้บริการธุรกรรมหรือให้สิทธิในการเข้าใช้งานระบบแก่บุคคลที่ไม่ถูกต้อง

ด้วยเหตุนี้ ผู้ให้บริการจึงต้องประเมินความเสี่ยงของการพิสูจน์ตัวตนที่ผิดพลาดและการยืนยันตัวตนที่ผิดพลาด เพื่อให้สามารถกำหนดระดับความน่าเชื่อถือที่เหมาะสมกับแต่ละบริการธุรกรรม และกำหนดกระบวนการและเทคโนโลยีที่จะใช้ให้เป็นไปตามระดับความน่าเชื่อถือแต่ละระดับ

4.2 ระดับความน่าเชื่อถือ

ผู้ให้บริการควรกำหนดระดับความน่าเชื่อถือ (assurance level) ของการพิสูจน์ตัวตนและการยืนยันตัวตนสำหรับแต่ละบริการธุรกรรมตามความเสี่ยงของบริการธุรกรรมนั้น มาตรฐานฉบับนี้แบ่งระดับความน่าเชื่อถือเป็น 2 ด้าน ดังนี้

(1) ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน คือ ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของบุคคล การกำหนดระดับ IAL ที่เหมาะสมจะช่วยลดโอกาสของการพิสูจน์ตัวตนที่ผิดพลาด โดยระดับ IAL แบ่งออกเป็น 3 ระดับ คือ IAL1 (ความน่าเชื่อถือต่ำที่สุด) IAL2 และ IAL3 (ความน่าเชื่อถือสูงที่สุด)

รายละเอียดเป็นไปตามมาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน

(2) ระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL)

ระดับความน่าเชื่อถือของการยืนยันตัวตน คือ ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตน การกำหนดระดับ AAL ที่เหมาะสมจะช่วยลดโอกาสของการยืนยันตัวตนที่ผิดพลาด โดยระดับ AAL แบ่งออกเป็น 3 ระดับ คือ AAL1 (ความน่าเชื่อถือต่ำที่สุด) AAL2 และ AAL3 (ความน่าเชื่อถือสูงที่สุด)

รายละเอียดเป็นไปตามมาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 3 ข้อกำหนดของการยืนยันตัวตน

4.3 การประเมินความเสี่ยงเพื่อกำหนดระดับความน่าเชื่อถือ

การประเมินความเสี่ยงเพื่อกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) ให้เหมาะสมกับแต่ละบริการธุรกรรม ประกอบด้วย 2 ขั้นตอน คือ (1) การประเมินระดับผลกระทบที่เป็นไปได้ และ (2) การเชื่อมโยงระดับผลกระทบที่เป็นไปได้เข้ากับระดับความน่าเชื่อถือ โดยมีรายละเอียดดังนี้

(1) ขั้นตอนที่ 1: การประเมินระดับผลกระทบที่เป็นไปได้

การประเมินระดับผลกระทบที่เป็นไปได้ (potential impact) เป็นการพิจารณาผลกระทบที่เป็นไปได้จากการพิสูจน์ตัวตนที่ผิดพลาด (สำหรับการกำหนดระดับ IAL) และผลกระทบที่เป็นไปได้จากการยืนยันตัวตนที่ผิดพลาด (สำหรับการกำหนดระดับ AAL)

ผู้ให้บริการควรประเมินความเสี่ยงและผลกระทบที่เป็นไปได้ของบริการธุรกรรม โดยพิจารณาให้เป็นไปตามหลักเกณฑ์ของหน่วยงานที่กำกับดูแลบริการธุรกรรมแต่ละประเภท นโยบายการบริหารความเสี่ยงของหน่วยงานของตนเอง และบริบทการใช้งานของบริการธุรกรรมนั้น อย่างไรก็ตาม ผู้ให้บริการอาจพิจารณาแบ่งประเภทของผลกระทบ (impact category) เป็น 6 ด้าน ดังนี้

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

การประเมินระดับผลกระทบที่เป็นไปได้จะใช้วิธีการพิจารณาระดับผลกระทบแต่ละด้านที่สามารถเป็นไปได้เมื่อเกิดข้อผิดพลาด ตามตารางที่ 1

ตารางที่ 1 เกณฑ์การประเมินระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด

ด้านของผลกระทบ	ระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด		
	ต่ำ	ปานกลาง	สูง
ความไม่สะดวกสบายและเสื่อมเสียชื่อเสียง	มีความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียงในระยะสั้นและจำกัด	มีความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียงรุนแรงระยะสั้น หรือมีผลปานกลางในระยะยาว	มีความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียงระยะยาว หรือมีผลกระทบหลายบุคคล
ความเสียหายทางการเงิน	มีความเสียหายทางการเงินที่ไม่มีนัยสำคัญ	มีความเสียหายทางการเงินรุนแรง	มีความเสียหายทางการเงินรุนแรงมาก
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบที่จำกัดต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงมากต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	มีการปล่อยข้อมูลส่วนบุคคลหรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับต่ำ	มีการปล่อยข้อมูลส่วนบุคคลหรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับปานกลาง	มีการปล่อยข้อมูลส่วนบุคคลหรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับสูง

ด้านของผลกระทบ	ระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด		
	ต่ำ	ปานกลาง	สูง
ความปลอดภัยของบุคคล	บาดเจ็บเล็กน้อย ไม่ต้องรับการรักษาพยาบาล	มีความเสี่ยงพอสมควรที่จะบาดเจ็บเล็กน้อย หรือมีความเสี่ยงจำกัดที่จะบาดเจ็บซึ่งต้องรับการรักษาพยาบาล	มีความเสี่ยงที่จะบาดเจ็บสาหัส หรือถึงแก่ชีวิต
การละเมิดทางแพ่งหรือทางอาญา	การฝ่าฝืนกฎหมายนั้นเป็นเรื่องเล็กน้อย ซึ่งไม่จำเป็นต้องมีการบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงที่จะถูกบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงสูงที่จะถูกบังคับใช้กฎหมาย

(2) ขั้นตอนที่ 2: การเชื่อมโยงระดับผลกระทบที่เป็นไปได้เข้ากับระดับความน่าเชื่อถือ

ผลการประเมินระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาดในการพิสูจน์ตัวตนและการยืนยันตัวตนจากขั้นตอนที่ 1 จะนำมาเชื่อมโยงเข้ากับระดับความน่าเชื่อถือ IAL และ AAL ตามลำดับ โดยระดับความน่าเชื่อถือ IAL และ AAL ที่เหมาะสมคือระดับที่ครอบคลุมผลกระทบที่เป็นไปได้ทุกด้านตามตารางที่ 2

ตารางที่ 2 ระดับผลกระทบที่เป็นไปได้และระดับความน่าเชื่อถือที่ต้องการ

ด้านของผลกระทบ	ระดับความน่าเชื่อถือที่ต้องการ		
	1	2	3
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

4.4 ตัวอย่างการกำหนดระดับความน่าเชื่อถือ

ตัวอย่างการกำหนดระดับความน่าเชื่อถือ IAL และ AAL ของ RP มีขั้นตอนดังนี้

(1) การกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL)

(1.1) ขั้นตอนที่ 1: การประเมินระดับผลกระทบที่เป็นไปได้จากการพิสูจน์ตัวตนที่ผิดพลาด โดยมีตัวอย่างของผลการประเมิน ดังนี้

ด้านของผลกระทบ	ระดับผลกระทบ
ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง	ต่ำ
ความเสียหายทางการเงิน	ต่ำ
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	ไม่มี
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	ไม่มี
ความปลอดภัยของบุคคล	ไม่มี
การละเมิดทางแพ่งหรือทางอาญา	ไม่มี

(1.2) ขั้นตอนที่ 2: การเชื่อมโยงผลระดับผลกระทบที่เป็นไปได้เข้ากับระดับความน่าเชื่อถือ

ด้านของผลกระทบ	ระดับความน่าเชื่อถือที่ต้องการ		
	1	2	3
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

จากการเชื่อมโยงระดับผลกระทบที่เป็นไปได้ (จากขั้นตอนที่ 1) เข้ากับระดับความน่าเชื่อถือ พบว่า ระดับความน่าเชื่อถือที่ครอบคลุมผลกระทบที่เป็นไปได้ทุกด้าน คือ ระดับ 1 ดังนั้น ระดับความน่าเชื่อถือ IAL ที่เหมาะสมในตัวอย่างนี้ คือ ระดับ IAL1

(2) การกำหนดระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL)

(2.1) ขั้นตอนที่ 1: การประเมินระดับผลกระทบที่เป็นไปได้จากการยืนยันตัวตนที่ผิดพลาด โดยมีตัวอย่างของผลการประเมิน ดังนี้

ด้านของผลกระทบ	ระดับผลกระทบ
ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง	ต่ำ
ความเสียหายทางการเงิน	ต่ำ
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	ต่ำ
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	ปานกลาง
ความปลอดภัยของบุคคล	ไม่มี
การละเมิดทางแพ่งหรือทางอาญา	ต่ำ

(2.2) ขั้นตอนที่ 2: การเชื่อมโยงระดับผลกระทบที่เป็นไปได้เข้ากับระดับความน่าเชื่อถือ

ด้านของผลกระทบ	ระดับความน่าเชื่อถือที่ต้องการ		
	1	2	3
ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง	ต่ำ	ปานกลาง	สูง
ความเสียหายทางการเงิน	ต่ำ	ปานกลาง	สูง
ความเสียหายต่อการดำเนินงานขององค์กร หรือต่อผลประโยชน์สาธารณะ	ไม่มี	ต่ำ/ปานกลาง	สูง
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	ไม่มี	ต่ำ/ปานกลาง	สูง
ความปลอดภัยของบุคคล	ไม่มี	ต่ำ	ปานกลาง/สูง
การละเมิดทางแพ่งหรือทางอาญา	ไม่มี	ต่ำ/ปานกลาง	สูง

จากการเชื่อมโยงระดับผลกระทบที่เป็นไปได้ (จากขั้นตอนที่ 1) เข้ากับระดับความน่าเชื่อถือ พบว่า ระดับความน่าเชื่อถือที่ครอบคลุมผลกระทบที่เป็นไปได้ทุกด้าน คือ ระดับ 2 ดังนั้น ระดับความน่าเชื่อถือ AAL ที่เหมาะสมในตัวอย่างนี้ คือ ระดับ AAL2

ภาคผนวก ก. อักษรย่อ

อักษรย่อ	คำเต็ม	คำภาษาไทย
IdP	identity provider	ผู้พิสูจน์และยืนยันตัวตน
RP	relying party	ผู้อาศัยการยืนยันตัวตน
AS	authoritative source	แหล่งข้อมูลที่น่าเชื่อถือ
IAL	identity assurance level	ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน
AAL	authentication assurance level	ระดับความน่าเชื่อถือของการยืนยันตัวตน
PIN	personal identification number	เลขรหัสส่วนตัว
OTP	one-time password	รหัสผ่านใช้ครั้งเดียว
FMR	false match rate	อัตราการเข้าคู่ผิดพลาด
FNMR	false non-match rate	อัตราการไม่เข้าคู่ผิดพลาด

บรรณานุกรม

[1] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม.

[2] พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. 2565.

[3] National Institute of Standards and Technology, U.S. Department of Commerce, "NIST Special Publication 800-63-3, Digital Identity Guidelines", June 2017.

[4] International Organization for Standardization, "ISO/IEC 29115:2013 Information technology – Security techniques – Entity authentication assurance framework", April 2013.

[5] Digital Transformation Agency, Australian Government, "Trusted Digital Identity Framework (TDIF): 01 - Glossary of Abbreviations and Terms", Release 4.6, March 2022.

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

ELECTRONIC TRANSACTION STANDARD

มธอ. 11 เล่ม 2-2569

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 2: ข้อกำหนดของการพิสูจน์ตัวตน

DIGITAL IDENTITY –
PART 2: IDENTITY PROOFING REQUIREMENTS

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.030

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 2: ข้อกำหนดของการพิสูจน์ตัวตน

มธอ. 11 เล่ม 2-2569

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ศูนย์ราชการเฉลิมพระเกียรติฯ (อาคารซี) ชั้นที่ 4 เลขที่ 120 หมู่ที่ 3 ซอยแจ้งวัฒนะ 7
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร 10210
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ประธานกรรมการ

นางวิลาวรรณ มังคละธนะกุล

รองประธานกรรมการ

นายพชร อนันตศิลป์ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

กรรมการผู้ทรงคุณวุฒิ

นายกอบศักดิ์ ดวงดี
นายทวีลาภ ฤทธาภิรมย์
นางปิยนุช วุฒิสอน
นายศักรินทร์ ร่วมรังษี
นายเฉลิมรัฐ นาควิเชียร
นายสุพันธุ์ ตั้งจิตกุศลมั่น
นางสาวอ้อนฟ้า เวชชาชีวะ

กรรมการและเลขานุการ

นายชัยชนะ มิตรพันธ์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คณะอนุกรรมการกลั่นกรองการกำหนดหลักเกณฑ์ในการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ประธานอนุกรรมการ

นางสาวอัจฉรินทร์ พัฒนพันธ์ชัย

อนุกรรมการ

นายอารยะ ไข่มุกด์	สำนักงานปลัดกระทรวงสาธารณสุข
นางสาวสุชาดา คำวงษ์	กรมการปกครอง
นายพลากรณ์ พูลเพิ่ม	กรมการกงสุล
นางศิริพร ชำนาญชาติ	กรมพัฒนาธุรกิจการค้า
นายพรรคธาดา ตรีรัตนพิทักษ์	ธนาคารแห่งประเทศไทย
นางสาวสายชล แซ่ลี้	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
นางสาวอรวรี เจริญพร	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
นายสมเกียรติ วัฒนาประสบสุข	สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
นายเฉลิมศักย์ ดาสะอาด	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
นายวิบูลย์ ภัทรพิบูล	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
นายสรรเพชร แสงเนตรสว่าง	สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายปรนนท์ ฐิตะวรรโณ	คณะกรรมการร่วมภาคเอกชน ๓ สถาบัน
นายวิเชียร เปรมชัยสวัสดิ์	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นายเฉลิมรัฐ นาควิเชียร	

เลขานุการ

นางสาวพิชญลักษณ์ เอกะพยัคฆ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คำนำ

ด้วยการเข้าทำธุรกรรมต่าง ๆ จำเป็นต้องมีกระบวนการพิสูจน์และยืนยันตัวตนผู้ที่ประสงค์จะเข้าทำธุรกรรมก่อนเพื่อให้มั่นใจได้ว่าผู้ที่ประสงค์จะเข้าทำธุรกรรมเป็นบุคคลนั้นจริง ประกอบกับในปัจจุบันมีการทำธุรกรรมและการให้บริการในรูปแบบดิจิทัลเพิ่มมากขึ้น ผู้ให้บริการจึงเริ่มมีการพัฒนากระบวนการพิสูจน์และยืนยันตัวตนทางดิจิทัลเพื่ออำนวยความสะดวกในการเข้าใช้บริการต่าง ๆ ในขณะเดียวกันกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ได้มีการแก้ไขปรับปรุงเพื่อรองรับให้บุคคลสามารถพิสูจน์และยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ ซึ่งกลไกดังกล่าวสามารถลดภาระต่อผู้ใช้บริการในการแสดงตน การส่งเอกสารหรือหลักฐานประกอบการพิสูจน์และยืนยันตัวตน รวมถึงช่วยลดขั้นตอนที่ต้องทำกระบวนการเดิมซ้ำ ๆ เพื่อพิสูจน์ตัวตนก่อนเข้าทำธุรกรรม

อย่างไรก็ตาม กระบวนการพิสูจน์และยืนยันตัวตนในปัจจุบันยังมีความหลากหลายและมีข้อกำหนดแตกต่างกันไปตามเงื่อนไขและความจำเป็นของผู้ให้บริการหรือหน่วยงานแต่ละแห่งซึ่งในบางกรณีอาจเกิดความไม่สอดคล้องหรือไม่สามารถนำมาใช้งานร่วมกันได้ ดังนั้น จึงได้มีการพัฒนามาตรฐานเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยการดำเนินการที่ผ่านมาสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชนได้ร่วมกันจัดทำมาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัล ได้แก่ ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ (ETDA Recommendation) ซึ่งมีการพัฒนาและปรับปรุงมาอย่างต่อเนื่อง ดังนี้

- เวอร์ชัน 1.0: เลขที่ ขมธอ. 18-2561, 19-2561 และ 20-2561
- เวอร์ชัน 2.0: เลขที่ ขมธอ. 18-2564, 19-2564 และ 20-2564
- เวอร์ชัน 3.0: เลขที่ ขมธอ. 18-2566, 19-2566 และ 20-2566

ในการนี้ เพื่อให้เกิดความสอดคล้องและเสริมสร้างความน่าเชื่อถือและยอมรับในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล และเพื่อให้ผู้ให้บริการและหน่วยงานต่าง ๆ สามารถใช้อ้างอิงและเลือกใช้งานดิจิทัลไอดีร่วมกันได้บนมาตรฐานและระดับความน่าเชื่อถือที่มีความสอดคล้องกัน คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงเห็นควรให้มีการยกระดับมาตรฐานดังกล่าว โดยนำข้อเสนอแนะมาตรฐานฯ เลขที่ ขมธอ. 18-2566, 19-2566 และ 20-2566 มาปรับปรุงเป็นชุดมาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล (เลขที่ มธอ. 11) ซึ่งประกอบด้วย

- เล่ม 1 กรอบการทำงาน (Part 1: Framework)
- เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน (Part 2: Identity Proofing Requirements)
- เล่ม 3 ข้อกำหนดของการยืนยันตัวตน (Part 3: Authentication Requirements)

สำหรับการพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน ฉบับนี้ เป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการพิสูจน์ตัวตนของบุคคลที่ประสงค์จะใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้ IdP มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกันตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ เลขที่ มธอ. 11 เล่ม 2-2566 ได้ถูกยกเลิกและแทนที่ด้วยมาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ เลขที่ มธอ. 11 เล่ม 2-2569 ฉบับนี้ ซึ่งพัฒนาต่อยอดจากฉบับเดิม โดยมีการปรับปรุงเนื้อหาทางเทคนิคให้มีความชัดเจนยิ่งขึ้น เพิ่มความสะดวกในการใช้งาน และสอดคล้องกับแนวปฏิบัติในปัจจุบัน

สารบัญ

หน้า

1. ขอบข่าย **1**

2. การพิสูจน์ตัวตน **1**

2.1 การรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ 1

2.2 การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ 2

2.3 การตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์ 2

3. ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL) **2**

3.1 ระดับ IAL1 2

3.2 ระดับ IAL2 2

3.3 ระดับ IAL3 3

4. ข้อกำหนดของการพิสูจน์ตัวตน **3**

4.1 ข้อกำหนดของการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ 3

4.2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ 4

4.3 ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์ 6

4.3.1 ข้อกำหนดของการเปรียบเทียบข้อมูลชีวมิติ 7

4.3.2 ข้อกำหนดของการเปรียบเทียบข้อมูลชีวมิติ กรณีใช้บริการระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (face verification service: FVS) ของกรมการปกครอง 7

4.4 สรุปข้อกำหนดที่สำคัญของการพิสูจน์ตัวตนตามระดับ IAL 8

ภาคผนวก ก. อินโฟกราฟิกส์ของระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) **12**

บรรณานุกรม **13**

สารบัญตาราง

หน้า

ตารางที่ 1 ข้อกำหนดของการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ 3

ตารางที่ 2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ 4

ตารางที่ 3 ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์ 6

ตารางที่ 4 สรุปข้อกำหนดที่สำคัญของการพิสูจน์ตัวตนตามระดับ IAL 9

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 2: ข้อกำหนดของการพิสูจน์ตัวตน

1. ขอบข่าย

มาตรฐานฉบับนี้เป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการพิสูจน์ตัวตนของบุคคลที่ประสงค์จะใช้บริการหรือทำธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้ IdP มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกันตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)

มาตรฐานฉบับนี้เป็นข้อกำหนดสำหรับหน่วยงานที่ให้บริการพิสูจน์และยืนยันตัวตนแก่บุคคลภายนอก ข้อกำหนดในมาตรฐานฉบับนี้สามารถประยุกต์ใช้ได้กับบริการพิสูจน์และยืนยันตัวตนที่ใช้เพื่อประโยชน์ภายในกิจการของตนเอง ทั้งนี้ ไม่มีเจตนาปิดกั้นหรือห้ามใช้วิธีการอื่นเพื่อเพิ่มประสิทธิภาพของการพิสูจน์และยืนยันตัวตน

มาตรฐานฉบับนี้มีรูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) ดังต่อไปนี้

- “ต้อง” (shall) ใช้ระบุสิ่งที่เป็นข้อกำหนด (requirement) ซึ่งต้องปฏิบัติตาม
- “ควร” (should) ใช้ระบุสิ่งที่เป็นข้อแนะนำ (recommendation)
- “อาจ” (may) ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้ (permission)

2. การพิสูจน์ตัวตน

การพิสูจน์ตัวตน (identity proofing) เป็นกระบวนการที่ IdP รวบรวมและตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคล และตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์นั้น โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าอัตลักษณ์ที่กล่าวอ้างเป็นอัตลักษณ์ของบุคคลนั้นจริงตามระดับความน่าเชื่อถือที่กำหนด โดยผลลัพธ์ที่คาดหวังจากการพิสูจน์ตัวตนของบุคคลที่ประสงค์จะมีดิจิทัลไอดีสำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ประกอบด้วย

- สามารถแยกแยะอัตลักษณ์ที่กล่าวอ้างว่าอัตลักษณ์นั้นมีเพียงอันเดียวและมีความเฉพาะเจาะจงในบริบทของบริการธุรกรรม
- สามารถตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ว่ามีความถูกต้อง แท้จริง และเป็นปัจจุบัน
- สามารถตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับข้อมูลเกี่ยวกับอัตลักษณ์ที่กล่าวอ้าง

การพิสูจน์ตัวตนประกอบด้วยกระบวนการพื้นฐาน 3 กระบวนการ ดังนี้ [1]

2.1 การรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์

การรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ คือ กระบวนการที่ IdP รวบรวมข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตน เพื่อใช้แยกแยะว่าอัตลักษณ์ที่กล่าวอ้างมีเพียงอันเดียวและมีความเฉพาะเจาะจงภายในบริบทของบริการธุรกรรม

2.2 การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์

การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ คือ กระบวนการที่ IdP ตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบันของข้อมูลเกี่ยวกับอัตลักษณ์ เพื่อพิสูจน์ว่าอัตลักษณ์ที่กล่าวอ้างเป็นข้อมูลของบุคคลที่มีอยู่จริง

2.3 การตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์

การตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์ คือ กระบวนการที่ IdP ตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับข้อมูลเกี่ยวกับอัตลักษณ์ที่กล่าวอ้าง เพื่อพิสูจน์ว่าบุคคลที่กำลังพิสูจน์ตัวตนเป็นเจ้าของข้อมูลเกี่ยวกับอัตลักษณ์ดังกล่าวจริง

หลังจากพิสูจน์ตัวตนเรียบร้อยแล้ว IdP จะเชื่อมโยงอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้ยืนยันตัวตน (authenticator) โดยบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วจะเปลี่ยนสถานะเป็นผู้ใช้บริการ และได้รับสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ในการยืนยันตัวตนต่อไป

3. ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL)

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL) คือ ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของบุคคล โดยระดับ IAL แบ่งออกเป็น 3 ระดับ ดังนี้

3.1 ระดับ IAL1

ระดับ IAL1 อาจมีการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ ซึ่งเป็นข้อมูลที่บุคคลยืนยันด้วยตนเอง (self-asserted) อย่างไรก็ตาม IAL1 อาจมีการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์หรือการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์ด้วยวิธีการอื่น ๆ ตามความเสี่ยงของบริการธุรกรรม นอกเหนือจากวิธีการที่กำหนดไว้ในระดับ IAL2 และ IAL3 เช่น

- ตรวจสอบสำเนาหรือรูปถ่ายของหลักฐานแสดงตน [1]
- ตรวจสอบลักษณะทางกายภาพของหลักฐานแสดงตนโดยเจ้าหน้าที่
- ตรวจสอบข้อมูลของหลักฐานแสดงตนและตรวจสอบสถานะของหลักฐานแสดงตน
- เปรียบเทียบใบหน้าหรือภาพใบหน้าของบุคคลกับภาพใบหน้าของหลักฐานแสดงตน
- ยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ (เช่น หมายเลขโทรศัพท์ อีเมล)

3.2 ระดับ IAL2

ระดับ IAL2 กำหนดให้มีการขอหลักฐานแสดงตน การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ว่าอัตลักษณ์ที่กล่าวอ้างเป็นข้อมูลของบุคคลที่มีอยู่จริง และการตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตน

[1] กรณีบัตรประจำตัวประชาชนแบบอเนกประสงค์ ควรจัดเก็บสำเนาหรือรูปถ่ายบัตรประจำตัวประชาชนเฉพาะด้านหน้าเพียงด้านเดียวตามคำแนะนำของกระทรวงมหาดไทย [5] ไม่ควรจัดเก็บสำเนาหรือรูปถ่ายของด้านหลังบัตรประจำตัวประชาชน เนื่องจากหมายเลขหลังบัตรประจำตัวประชาชน (laser code) เป็นข้อมูลที่อาจใช้ในการยืนยันตัวตนหรือทำธุรกรรมในบางกรณี หากมีการรั่วไหลของข้อมูลดังกล่าว อาจจะทำให้เกิดความเสียหายต่อผู้ใช้บริการ

กับข้อมูลเกี่ยวกับอัตลักษณ์นั้น ทั้งนี้ การพิสูจน์ตัวตนที่ระดับ IAL2 สามารถทำได้ทั้งแบบพบเห็นต่อหน้า (face-to-face) หรือแบบไม่พบเห็นต่อหน้า (non face-to-face) เช่น การพิสูจน์ตัวตนผ่านเครื่องให้บริการ (kiosk) หรือแอปพลิเคชันของ IdP

IdP ที่รองรับระดับ IAL2 สามารถส่งผลการยืนยันตัวตนที่มีข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลนั้นให้กับ RP ที่ต้องการระดับ IAL เท่ากันหรือต่ำกว่าได้ หากได้รับความยินยอมจากบุคคลที่เป็นเจ้าของข้อมูล

ในทางปฏิบัติ ระดับ IAL2 จะแบ่งออกเป็น 3 ระดับย่อย คือ IAL2.1, IAL2.2 และ IAL2.3 โดยพิจารณาจากความเข้มงวดของวิธีการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์และวิธีการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์

3.3 ระดับ IAL3

ระดับ IAL3 เพิ่มความเข้มงวดจากระดับ IAL2 โดยกำหนดให้มีการตรวจสอบความมีอยู่จริงของอัตลักษณ์จากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติม และการตรวจสอบความเชื่อมโยงระหว่างบุคคลที่กำลังพิสูจน์ตัวตนกับข้อมูลเกี่ยวกับอัตลักษณ์ด้วยการเปรียบเทียบข้อมูลชีวมิติ (biometric comparison) เพื่อป้องกันการปลอมตัวเป็นบุคคลอื่นและการลงทะเบียนซ้ำ ทั้งนี้ การพิสูจน์ตัวตนที่ระดับ IAL3 ต้องทำแบบพบเห็นต่อหน้า (face-to-face) เท่านั้น

IdP ที่รองรับระดับ IAL3 สามารถส่งผลการยืนยันตัวตนที่มีข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลนั้นให้กับ RP ที่ต้องการระดับ IAL เท่ากันหรือต่ำกว่าได้ หากได้รับความยินยอมจากบุคคลที่เป็นเจ้าของข้อมูล

4. ข้อกำหนดของการพิสูจน์ตัวตน

4.1 ข้อกำหนดของการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์

ข้อกำหนดของการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ตามระดับ IAL สามารถแสดงได้ตามตารางที่ 1

ตารางที่ 1 ข้อกำหนดของการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์

ระดับ IAL	ข้อกำหนดของการรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์
IAL1	(1) IdP อาจรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ ซึ่งเป็นข้อมูลที่บุคคลยืนยันด้วยตนเอง (self-asserted) เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจง
IAL2	(1) IdP ต้องรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตนอย่างน้อย 1 ฉบับ เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจง (2) IdP ที่รองรับระดับ IAL2 สามารถส่งข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลให้กับ RP ที่ต้องการระดับ IAL เท่ากันหรือต่ำกว่าได้ หากได้รับความยินยอมจากบุคคลที่เป็นเจ้าของข้อมูล
IAL3	(1) IdP ต้องรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตนอย่างน้อย 1 ฉบับ และจากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติม (นอกเหนือจากฐานข้อมูลทะเบียนของกรมการปกครอง) เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจง (2) IdP ที่รองรับระดับ IAL3 สามารถส่งข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลให้กับ RP ที่ต้องการระดับ IAL เท่ากันหรือต่ำกว่าได้ หากได้รับความยินยอมจากบุคคลที่เป็นเจ้าของข้อมูล

4.2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์

ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ตามระดับ IAL สามารถแสดงได้ตามตารางที่ 2

ตารางที่ 2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์

ระดับ IAL	ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์
IAL1	IdP ไม่จำเป็นต้องตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์
IAL2.1	<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์เป็นหลักฐานแสดงตน</u> (1) กรณีมีเครื่องอ่านบัตรประจำตัวประชาชน IdP <u>ต้อง</u>ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตรประจำตัวประชาชน เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของบัตรประจำตัวประชาชน (2) กรณีไม่มีเครื่องอ่านบัตรประจำตัวประชาชน IdP <u>ต้อง</u>ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ โดยใช้ข้อมูลจากผลการยืนยันตัวตนผ่าน IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 ขึ้นไป ทั้งนี้ การส่งผลการยืนยันตัวตนที่มีข้อมูลเกี่ยวกับอัตลักษณ์ต้องให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย (3) IdP <u>ควร</u>ตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล <u>กรณีใช้หนังสือเดินทางเป็นหลักฐานแสดงตน</u> (1) IdP <u>ต้อง</u>ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เทคโนโลยีสื่อสารไร้สายระยะใกล้ (near field communication: NFC) เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของหนังสือเดินทาง (2) IdP <u>ควร</u>ตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล
IAL2.2	<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์เป็นหลักฐานแสดงตน</u> (1) กรณีมีเครื่องอ่านบัตรประจำตัวประชาชน IdP <u>ต้อง</u>ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตรประจำตัวประชาชน เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของบัตรประจำตัวประชาชน (2) กรณีไม่มีเครื่องอ่านบัตรประจำตัวประชาชน IdP <u>ต้อง</u>ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ โดยใช้ข้อมูลจากผลการยืนยันตัวตนผ่าน IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 ขึ้นไป ทั้งนี้ การส่งผลการยืนยันตัวตนที่มีข้อมูลเกี่ยวกับอัตลักษณ์ต้องให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย (3) IdP <u>ต้อง</u>ตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ โดยใช้หมายเลขชิป (chip number) กรณีมีเครื่องอ่านบัตรประจำตัวประชาชน หรือใช้หมายเลขหลังบัตรประจำตัวประชาชน (laser code) กรณีไม่มีเครื่องอ่านบัตรประจำตัวประชาชน

ระดับ IAL	ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์
	(4) IdP ควรตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล กรณีใช้หนังสือเดินทางเป็นหลักฐานแสดงตน (1) IdP ต้องตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เทคโนโลยีสื่อสารไร้สายระยะใกล้ (NFC) เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของหนังสือเดินทาง (2) IdP ต้องตรวจสอบสถานะของหนังสือเดินทางด้วยแหล่งข้อมูลที่น่าเชื่อถือ หรือตรวจสอบเอกสารสำคัญประจำตัวอื่นที่รัฐบาลไทยหรือหน่วยงานของรัฐเจ้าของสัญชาติออกให้ (เช่น ใบอนุญาตทำงาน ใบขับขี่) หรือตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ โดยใช้หมายเลขหลังบัตรประจำตัวประชาชน (laser code) (3) IdP ควรตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล
IAL2.3	กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์เป็นหลักฐานแสดงตน (1) กรณีมีเครื่องอ่านบัตรประจำตัวประชาชน IdP ต้องตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตรประจำตัวประชาชน เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของบัตรประจำตัวประชาชน และตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ โดยใช้หมายเลขชิป (chip number) (2) กรณีไม่มีเครื่องอ่านบัตรประจำตัวประชาชน IdP ต้องได้รับอนุญาตให้ใช้บริการระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (face verification service) ของกรมการปกครอง [2] โดย IdP ต้องตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ด้วยการยืนยันตัวตนเจ้าของข้อมูลตามหลักเกณฑ์หรือวิธีการที่กรมการปกครองกำหนด (3) IdP ควรตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล กรณีใช้หนังสือเดินทางเป็นหลักฐานแสดงตน ข้อกำหนดเช่นเดียวกับ IAL2.2

[2] ระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (face verification service: FVS) คือ ระบบที่กรมการปกครองได้จัดสร้างและพัฒนาขึ้น เพื่อให้บริการเปรียบเทียบ (matching) ข้อมูลชีวมิติจากภาพใบหน้าของบุคคล กับข้อมูลภาพใบหน้าของบุคคลดังกล่าวในฐานข้อมูลทะเบียนประวัติราษฎรของสำนักทะเบียนกลางแบบหนึ่งต่อหนึ่ง (one-to-one) โดยการแจ้งผลการเปรียบเทียบแก่ผู้ใช้บริการในรูปแบบคะแนนความเหมือนเป็นร้อยละ (match score) เพื่อวัตถุประสงค์ในการพิสูจน์ตัวตนของบุคคล [6]

ระดับ IAL	ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์
IAL3	กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์เป็นหลักฐานแสดงตน (1) IdP ต้องตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตรประจำตัวประชาชน เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของบัตรประจำตัวประชาชน และตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ โดยใช้หมายเลขชิป (chip number) (2) IdP ต้องตรวจสอบความมีอยู่จริงของอัตลักษณ์จากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติมอย่างน้อย 1 หน่วยงาน นอกเหนือจากฐานข้อมูลทะเบียนของกรมการปกครอง (3) IdP ควรตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล

4.3 ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์

ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์ตามระดับ IAL สามารถแสดงได้ตามตารางที่ 3

ตารางที่ 3 ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์

ระดับ IAL	ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์
IAL1	IdP ไม่จำเป็นต้องตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์
IAL2.1	(1) การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า**หรือ**แบบไม่พบเห็นต่อหน้า (2) IdP ต้องให้เจ้าหน้าที่เปรียบเทียบใบหน้าหรือภาพใบหน้าของบุคคล (visual comparison) กับภาพใบหน้าจากชิปของหลักฐานแสดงตนของหน่วยงานของรัฐ หรือภาพใบหน้าจาก IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 ขึ้นไป ทั้งนี้ การส่งภาพใบหน้าต้องให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย (3) กรณีพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า IdP ต้องบันทึกภาพใบหน้าของบุคคล เพื่อป้องกันการปฏิเสธว่าไม่ได้พิสูจน์ตัวตนหรือเพื่อใช้พิสูจน์ตัวตนอีกครั้ง
IAL2.2	ข้อกำหนดเช่นเดียวกับ IAL2.1
IAL2.3	(1) การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า**หรือ**แบบไม่พบเห็นต่อหน้า (2) IdP ต้องเปรียบเทียบข้อมูลชีวมิติ (biometric comparison) โดยใช้วิธีการใดวิธีการหนึ่ง ดังนี้ (2.1) IdP ใช้เทคโนโลยีชีวมิติในการเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของบุคคลกับข้อมูลชีวมิติจากชิปของหลักฐานแสดงตนของหน่วยงานของรัฐ (2.2) IdP ใช้ระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (face verification service) ของกรมการปกครองในการเปรียบเทียบภาพใบหน้าของบุคคลกับฐานข้อมูลชีวมิติ (3) กรณีพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า IdP ต้องบันทึกข้อมูลชีวมิติตั้งต้นของบุคคล (biometric sample) เพื่อป้องกันการปฏิเสธว่าไม่ได้พิสูจน์ตัวตนหรือเพื่อใช้พิสูจน์ตัวตนอีกครั้ง

ระดับ IAL	ข้อกำหนดของการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์
IAL3	(1) การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า**เท่านั้น** (2) IdP ต้องเปรียบเทียบข้อมูลชีวมิติ (biometric comparison) โดยใช้วิธีการใดวิธีการหนึ่ง ดังนี้ (2.1) IdP ใช้เทคโนโลยีชีวมิติในการเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของบุคคลกับข้อมูลชีวมิติจากชิปของหลักฐานแสดงตนของหน่วยงานของรัฐ (2.2) IdP ใช้ระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (face verification service) ของกรมการปกครองในการเปรียบเทียบภาพใบหน้าของบุคคลกับฐานข้อมูลชีวมิติ (3) IdP ต้องบันทึกข้อมูลชีวมิติตั้งต้นของบุคคล (biometric sample) เพื่อป้องกันการปฏิเสธว่าไม่ได้พิสูจน์ตัวตนหรือเพื่อใช้พิสูจน์ตัวตนอีกครั้ง

4.3.1 ข้อกำหนดของการเปรียบเทียบข้อมูลชีวมิติ

(1) การเปรียบเทียบข้อมูลชีวมิติต้องดำเนินการเปรียบเทียบแบบหนึ่งต่อหนึ่ง (one-to-one comparison) ระหว่างข้อมูลชีวมิติของบุคคลที่แสดงตนกับข้อมูลชีวมิติจากหลักฐานแสดงตนหรือจากหน่วยงานของรัฐ โดยไม่ทำการเปรียบเทียบแบบหนึ่งต่อกลุ่ม (one-to-many comparison) กับฐานข้อมูลที่มีข้อมูลชีวมิติของบุคคลมากกว่าหนึ่งคน

(2) ความแม่นยำในการเปรียบเทียบข้อมูลชีวมิติต้องมีอัตราการเข้าคู่ผิดพลาด (false match rate: FMR) ไม่เกิน 0.01% และอัตราการไม่เข้าคู่ผิดพลาด (false non-match rate: FNMR) ไม่เกิน 3% [2]

(3) กรณีการพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า IdP ต้องมีเทคโนโลยีการตรวจจับการโจมตีหลอกระบบ (presentation attack detection: PAD) เช่น การตรวจจับการมีชีวิต (liveness detection) เพื่อช่วยป้องกันการโจมตีด้วยการใช้ภาพใบหน้าหรือลายนิ้วมือปลอม (spoofing attack) ทั้งนี้ IdP สามารถพิจารณาการทดสอบความสามารถของเทคโนโลยีการตรวจจับการโจมตีหลอกระบบ (PAD) ให้สอดคล้องหรือเทียบเคียงได้ตามมาตรฐานสากล เช่น ISO/IEC 30107 Information technology – Biometric presentation attack detection หรือ FIDO Biometrics Requirements

4.3.2 ข้อกำหนดของการเปรียบเทียบข้อมูลชีวมิติ กรณีใช้บริการระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (face verification service: FVS) ของกรมการปกครอง

(1) IdP ต้องควบคุมการจัดเก็บ (capture) ภาพใบหน้าของบุคคล เพื่อใช้ในการเปรียบเทียบข้อมูลชีวมิติจากภาพใบหน้า ให้ดำเนินการโดยระบบของ IdP โดยตรงเท่านั้น

(2) IdP ต้องมีเทคโนโลยีการตรวจจับการโจมตีหลอกระบบ (presentation attack detection: PAD) เช่น การตรวจจับการมีชีวิต (liveness detection) เพื่อช่วยป้องกันการโจมตีด้วยการใช้ภาพใบหน้าหรือลายนิ้วมือปลอม (spoofing attack) ทั้งนี้ IdP สามารถพิจารณาการทดสอบความสามารถของเทคโนโลยีการตรวจจับการโจมตีหลอกระบบ (PAD) ให้สอดคล้องหรือเทียบเคียงได้ตามมาตรฐานสากล เช่น ISO/IEC 30107 Information technology – Biometric presentation attack detection หรือ FIDO Biometrics Requirements

(3) IdP ต้องควบคุมให้ภาพใบหน้าของบุคคลที่ได้จากการจัดเก็บจากระบบของหน่วยงาน มีคุณภาพดีตามที่กรมการปกครองกำหนด เพื่อให้การเปรียบเทียบข้อมูลชีวมิติจากภาพใบหน้าด้วยระบบ FVS มีประสิทธิภาพและมีความแม่นยำ ทั้งนี้ การควบคุมคุณภาพของภาพใบหน้า อย่างน้อยต้องคำนึงถึงชนิดของภาพ (ภาพสีหรือภาพระดับเทา) ขนาดภาพ ความละเอียดของภาพ และขนาดใบหน้าที่ปรากฏบนภาพ

(4) IdP ต้องจัดทำคำขอเปรียบเทียบภาพใบหน้า พร้อมด้วยข้อมูลเลขประจำตัวประชาชน และภาพใบหน้าของบุคคลที่จัดเก็บ เพื่อใช้ในการเปรียบเทียบภาพใบหน้ากับระบบ FVS

(5) IdP ต้องจัดทำรายละเอียดของกระบวนการควบคุมคุณภาพของภาพใบหน้า พร้อมหลักเกณฑ์และผลการพิจารณาของ IdP ในการพิจารณาผลเปรียบเทียบจากค่าคะแนนความเหมือนที่ได้รับแจ้งจากระบบ FVS เพื่อพิสูจน์ตัวตนของบุคคล

4.4 สรุปข้อกำหนดที่สำคัญของการพิสูจน์ตัวตนตามระดับ IAL

ข้อกำหนดที่สำคัญของการพิสูจน์ตัวตนตามระดับ IAL แต่ละระดับสามารถสรุปได้ตามตารางที่ 4

ตารางที่ 4 สรุปข้อกำหนดที่สำคัญของการพิสูจน์ตัวตนตามระดับ IAL

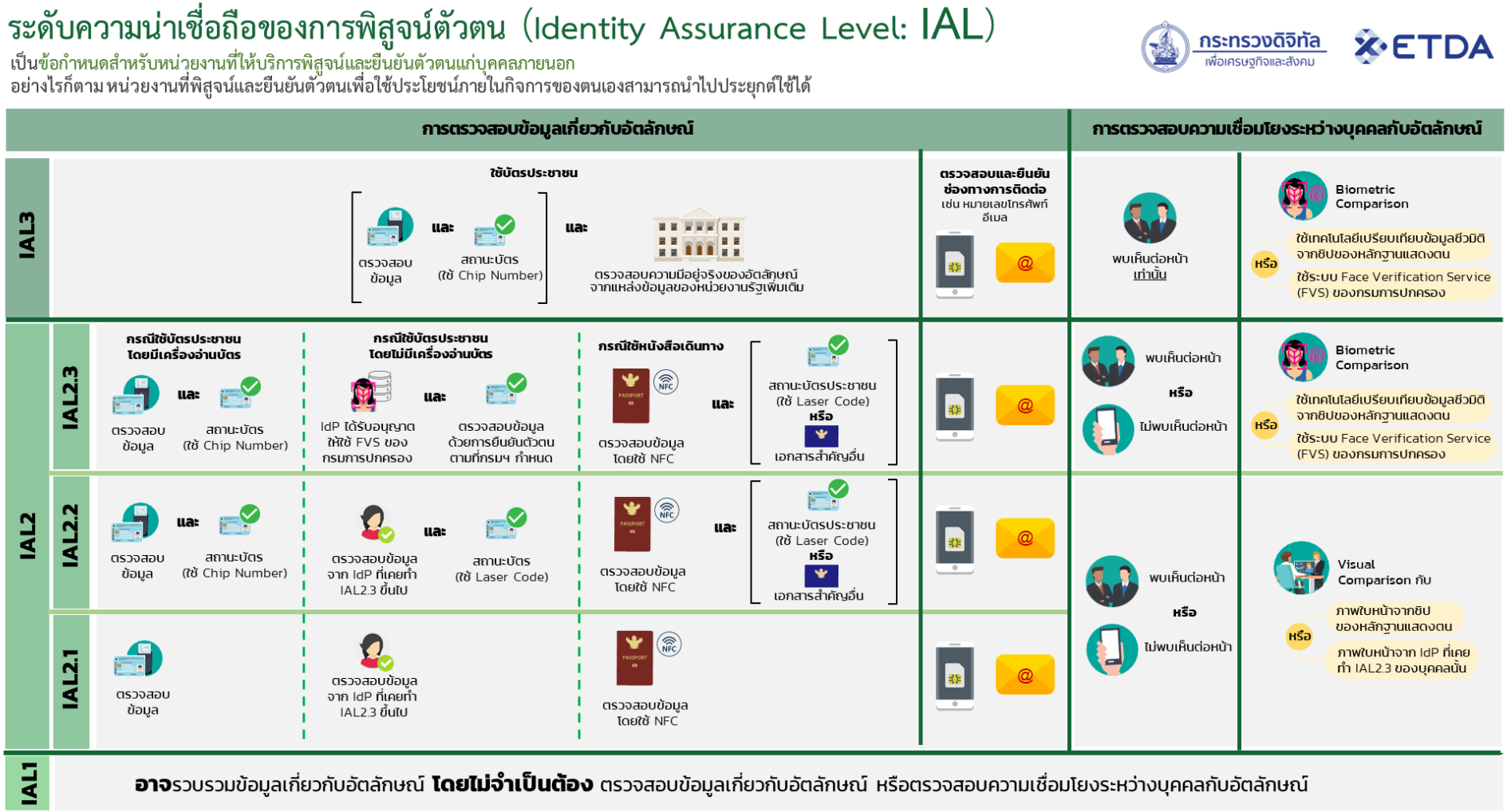
ข้อกำหนดของการพิสูจน์ตัวตน	การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า					การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า				
	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3
การรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์										
รวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ ซึ่งเป็นข้อมูลที่บุคคลยืนยันด้วยตนเอง (self-asserted) เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจง	✓ (อาจ)					✓ (อาจ)				
รวบรวมข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตนอย่างน้อย 1 ฉบับ เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจง		✓ (ต้อง)	✓ (ต้อง)	✓ (ต้อง)			✓ (ต้อง)	✓ (ต้อง)	✓ (ต้อง)	
รวบรวมข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตนอย่างน้อย 1 ฉบับ และจากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติม (นอกเหนือจากฐานข้อมูลทะเบียนของกรมการปกครอง) เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจง										✓ (ต้อง)
การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์										
<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์</u> – <u>กรณีมีเครื่องอ่านบัตร</u> ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตร เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของบัตรประจำตัวประชาชน – <u>กรณีไม่มีเครื่องอ่านบัตร</u> ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ โดยใช้ข้อมูลจากผลการยืนยันตัวตนผ่าน IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 ขึ้นไป ทั้งนี้ การส่งผลการยืนยันตัวตนที่มีข้อมูลเกี่ยวกับอัตลักษณ์ต้องให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย		✓ (ต้อง)	✓ (ต้อง)				✓ (ต้อง)	✓ (ต้อง)		
<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์</u> – ตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ โดยใช้หมายเลขชิป (chip number) กรณีมีเครื่องอ่านบัตร หรือใช้หมายเลขหลังบัตรประจำตัวประชาชน (laser code) กรณีไม่มีเครื่องอ่านบัตร			✓ (ต้อง)					✓ (ต้อง)		

ข้อกำหนดของการพิสูจน์ตัวตน	การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า					การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า				
	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3
<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์</u> – <u>กรณีมีเครื่องอ่านบัตร</u> ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตร เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของบัตรประจำตัวประชาชน และตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานรัฐ โดยใช้หมายเลขชิป (chip number) – <u>กรณีไม่มีเครื่องอ่านบัตร</u> IdP ต้องได้รับอนุญาตให้ใช้บริการระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (face verification service) ของกรมการปกครอง โดยตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ด้วยการยืนยันตัวตนเจ้าของข้อมูลตามหลักเกณฑ์หรือวิธีการที่กรมการปกครองกำหนด				✓ (ต้อง)					✓ (ต้อง)	
<u>กรณีใช้บัตรประจำตัวประชาชนแบบอเนกประสงค์</u> – ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เครื่องอ่านบัตร เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของบัตรประจำตัวประชาชน และตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานรัฐ โดยใช้หมายเลขชิป (chip number) – ตรวจสอบความมีอยู่จริงของอัตลักษณ์จากแหล่งข้อมูลที่น่าเชื่อถือของหน่วยงานของรัฐเพิ่มเติมอย่างน้อย 1 หน่วยงาน นอกเหนือจากฐานข้อมูลทะเบียนของกรมการปกครอง										✓ (ต้อง)
<u>กรณีใช้หนังสือเดินทาง</u> – ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์โดยใช้เทคโนโลยีสื่อสารไร้สายระยะใกล้ (NFC) เพื่อเปรียบเทียบข้อมูลเกี่ยวกับอัตลักษณ์กับข้อมูลจากชิปของหนังสือเดินทาง		✓ (ต้อง)	✓ (ต้อง)	✓ (ต้อง)			✓ (ต้อง)	✓ (ต้อง)	✓ (ต้อง)	
<u>กรณีใช้หนังสือเดินทาง</u> – ตรวจสอบสถานะของหนังสือเดินทางด้วยแหล่งข้อมูลที่น่าเชื่อถือ หรือตรวจสอบเอกสารสำคัญประจำตัวอื่นที่รัฐบาลไทยหรือหน่วยงานของรัฐเจ้าของสัญชาติออกให้ หรือตรวจสอบสถานะของบัตรประจำตัวประชาชนด้วยระบบตรวจสอบของหน่วยงานของรัฐ โดยใช้หมายเลขหลังบัตรประจำตัวประชาชน (laser code)			✓ (ต้อง)	✓ (ต้อง)				✓ (ต้อง)	✓ (ต้อง)	

ข้อกำหนดของการพิสูจน์ตัวตน	การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า					การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า				
	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3
ตรวจสอบและยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น ตรวจสอบหมายเลขโทรศัพท์กับผู้ให้บริการโทรศัพท์เคลื่อนที่ และยืนยันช่องทางการติดต่อด้วยรหัสผ่านใช้ครั้งเดียว (OTP) ที่ส่งให้ทาง SMS หรืออีเมล		✓ (ควร)	✓ (ควร)	✓ (ควร)			✓ (ควร)	✓ (ควร)	✓ (ควร)	✓ (ควร)
การตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์										
ให้เจ้าหน้าที่เปรียบเทียบใบหน้าหรือภาพใบหน้าของบุคคล (visual comparison) กับภาพใบหน้าจากชิปของหลักฐานแสดงตนของหน่วยงานของรัฐ หรือภาพใบหน้าจาก IdP ที่เคยพิสูจน์ตัวตนของบุคคลนั้นมาก่อนที่ระดับ IAL2.3 ขึ้นไป ทั้งนี้ การส่งภาพใบหน้าต้องให้บุคคลนั้นยืนยันตัวตนที่ระดับ AAL2 เป็นอย่างน้อย		✓ (ต้อง)	✓ (ต้อง)				✓ (ต้อง)	✓ (ต้อง)		
เปรียบเทียบข้อมูลชีวมิติ (biometric comparison) โดยใช้วิธีการใดวิธีการหนึ่ง ดังนี้ – IdP ใช้เทคโนโลยีชีวมิติในการเปรียบเทียบภาพใบหน้าหรือลายนิ้วมือของบุคคลกับข้อมูลชีวมิติจากชิปของหลักฐานแสดงตนของหน่วยงานของรัฐ – IdP ใช้ระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (face verification service) ของกรมการปกครองในการเปรียบเทียบภาพใบหน้าของบุคคลกับฐานข้อมูลชีวมิติ				✓ (ต้อง)					✓ (ต้อง)	✓ (ต้อง)
มีเทคโนโลยีการตรวจจับการโจมตีหลอกระบบ (presentation attack detection: PAD) เช่น การตรวจจับการมีชีวิต (liveness detection) เพื่อช่วยป้องกันการโจมตีด้วยการใช้ภาพใบหน้าหรือลายนิ้วมือปลอม (spoofing attack)				✓ (ต้อง)						
บันทึกภาพใบหน้าหรือข้อมูลชีวมิติตั้งต้นของบุคคล (biometric sample) เพื่อป้องกันการปฏิเสธว่าไม่ได้พิสูจน์ตัวตนหรือเพื่อใช้พิสูจน์ตัวตนอีกครั้ง		✓ (ต้อง)	✓ (ต้อง)	✓ (ต้อง)						✓ (ต้อง)

ภาคผนวก ก. อินโฟกราฟิกส์ของระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL)

อินโฟกราฟิกส์ (infographics) ของระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL) ซึ่งเป็นการสรุปข้อกำหนดที่สำคัญบางส่วนจากมาตรฐานเพื่อนำเสนอข้อมูลเป็นภาพที่สามารถเข้าใจได้ง่าย แสดงตามนี้



หมายเหตุ: เป็นการสรุปข้อกำหนดที่สำคัญบางส่วนจากมาตรฐาน

ศึกษารายละเอียดจาก มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน (เลขที่ มธอ. 11 เล่ม 2-2569)

บรรณานุกรม

[1] National Institute of Standards and Technology, U.S. Department of Commerce, "NIST Special Publication 800-63A, Digital Identity Guidelines: Enrollment and Identity Proofing", June 2017.

[2] Digital Transformation Agency, Australian Government, "Trusted Digital Identity Framework (TDIF): 05 - Role Requirements", Release 4.7, June 2022.

[3] International Organization for Standardization, "ISO/IEC 29115:2013 Information technology – Security techniques – Entity authentication assurance framework", April 2013.

[4] International Organization for Standardization, "ISO/IEC 30107-3:2017 Information technology – Biometric presentation attack detection – Part 3: Testing and reporting", September 2017.

[5] หนังสือกระทรวงมหาดไทย ที่ มท 0309.2/ว 6857 ลงวันที่ 22 มีนาคม 2556 เรื่อง การถ่ายสำเนาบัตรประจำตัวประชาชนแบบอเนกประสงค์ (Smart Card).

[6] ประกาศกรมการปกครอง เรื่อง หลักเกณฑ์การอนุญาตให้หน่วยงานของรัฐและหน่วยงานเอกชนใช้บริการระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (DOPA-Digital ID) และระบบพิสูจน์ตัวตนด้วยใบหน้าทางดิจิทัล (Face Verification Service : FVS) ของกรมการปกครอง, 18 มิถุนายน 2567.

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

ELECTRONIC TRANSACTION STANDARD

มธอ. 11 เล่ม 3-2566

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 3: ข้อกำหนดของการยืนยันตัวตน

DIGITAL IDENTITY –
PART 3: AUTHENTICATION REQUIREMENTS

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.030

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 3: ข้อกำหนดของการยืนยันตัวตน

มธอ. 11 เล่ม 3-2566

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 20-22
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ประธานกรรมการ

นางอรรชกา สีบุญเรือง

รองประธานกรรมการ

นายวิศิษฏ์ วิศิษฏ์สรอรรถ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

กรรมการผู้ทรงคุณวุฒิ

นางสาวสิริธิดา พนมวัน ณ อยุธยา
นายศีลวัต สันติวิสัฏฐ์
นายปณิธิ ชุณหสวัสดิกุล
นายอนุชิต อนุชิตานุกูล
นายกนิษฐ์ สารสิน
นางสาวช่อผกา วิริยานนท์
นายเฉลิมรัฐ นาควิเชียร
นายยรรยง เต็งอำนวย

กรรมการและเลขานุการ

นายชัยชนะ มิตรพันธ์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คณะอนุกรรมการกลั่นกรองการกำหนดหลักเกณฑ์ในการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ประธานอนุกรรมการ

นางสาวอัจฉรินทร์ พัฒนพันธ์ชัย

อนุกรรมการ

นายอนันต์ กนกศิลป์	สำนักงานปลัดกระทรวงสาธารณสุข
นางรุ่งนิภา อมาตยคง	
นายสัญชัย เตชนิมิตวัช	กรมการปกครอง
นายอภิวัฒน์ อินขัด	กรมการกงสุล
นางศิริพร ชำนาญชาติ	กรมพัฒนาธุรกิจการค้า
นางสาวรัญศิกานต์ งามบุษบงโสภา	
นางสาวสิริธิดา พนมวัน ณ อยุธยา	ธนาคารแห่งประเทศไทย
นางสาววิจิตรเลขา มารมย์	
นางสาวสายชล แซ่ลี้	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
นางสาวจิตสถา ศรีประเสริฐสุข	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และ
นางสาวอรวรี เจริญพร	กิจการโทรคมนาคมแห่งชาติ
นายสมเกียรติ วัฒนาประสบสุข	สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
นายณัฐวุฒิ ทิพย์กนก	
นายณรงค์เดช วัชระภาสร	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
นายกิตตินันท์ ศรีมงคล	
นายวิบูลย์ ภัทรพิบูล	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
นายอภิสิทธิ์ สุขสาคร	
นายพีรธร วิมลโลหการ	สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน
นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นางสาวอุรัชฎา เกตุพรหม	
นายจำรัส สว่างสมุทร	คณะกรรมการร่วมภาคเอกชน ๓ สถาบัน
นายวิเชียร เปรมชัยสวัสดิ์	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นายณัฐวุฒิ อมรวิวัฒน์	

เลขานุการ

นางสาวพลอย เจริญสม	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คณะอนุกรรมการมาตรฐานและการกำกับดูแล

ประธานอนุกรรมการ

นายยรรยง เต็งอำนวย

อนุกรรมการ

รองศาสตราจารย์ปริทรรศน์ พันธุบรรยงก์	
นายปริญญา หอมเอนก	
นางสาวภรณี หรูวรรธนะ	
นายรอม หิรัญพฤกษ์	
นางสาวสุธีรา ศรีไพบูลย์	
นายอนุชิต อนุชิตานุกูล	
นางสาวสุดจิตร ลาภเลิศสุข	กรมบัญชีกลาง
นางสาวภิญญู กำเนิดหล่ม	กรมสรรพากร
นางสาวรัญศิกานต์ งามบุษบงโสภา	กรมพัฒนาธุรกิจการค้า
นายก่อเกียรติ แก้วกิ่ง	กรมการปกครอง
นางศิริพร ช่างการ	สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม
นายสมเกียรติ วัฒนาประสบสุข	สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
นายกำพล ศรธนะรัตน์	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
นายเนติพงษ์ ตลับนาค	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
นายสินชัย ต่อวัฒนกิจกุล	สำนักงานหลักประกันสุขภาพแห่งชาติ
นางบุษกร ธีระปัญญาชัย	ธนาคารแห่งประเทศไทย
นายภิญโญ ตรีเพชราภรณ์	
นายเอธ แย้มประทุม	
นายสุพจน์ เธียรวุฒิ	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
นายวิบูลย์ ภัทรพิบูล	
นายวีระ วีระกุล	สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย
นางสาวธิดารัช ธนภรรคภวิน	

อนุกรรมการและเลขานุการ

นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ผู้ช่วยเลขานุการ

นายสิริณัฐ ตั้งธรรมจิต	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คำนำ

ด้วยการเข้าทำธุรกรรมต่าง ๆ จำเป็นต้องมีกระบวนการพิสูจน์และยืนยันตัวตนผู้ที่ประสงค์จะเข้าทำธุรกรรมก่อนเพื่อให้มั่นใจได้ว่าผู้ที่ประสงค์จะเข้าทำธุรกรรมเป็นบุคคลนั้นจริง ประกอบกับในปัจจุบันมีการทำธุรกรรมและการให้บริการในรูปแบบดิจิทัลเพิ่มมากขึ้น ผู้ให้บริการจึงเริ่มมีการพัฒนากระบวนการ พิสูจน์และยืนยันตัวตนทางดิจิทัลเพื่ออำนวยความสะดวกในการเข้าใช้บริการต่าง ๆ ในขณะเดียวกันกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ได้มีการแก้ไขปรับปรุงเพื่อรองรับให้บุคคลสามารถพิสูจน์และยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ ซึ่งกลไกดังกล่าวสามารถลดภาระต่อผู้ใช้บริการในการแสดงตน การส่งเอกสารหรือหลักฐานประกอบการพิสูจน์และยืนยันตัวตน รวมถึงช่วยลดขั้นตอนที่ต้องทำกระบวนการเดิมซ้ำ ๆ เพื่อพิสูจน์ตัวตนก่อนเข้าทำธุรกรรม

อย่างไรก็ตาม กระบวนการพิสูจน์และยืนยันตัวตนในปัจจุบันยังมีความหลากหลายและมีข้อกำหนดแตกต่างกันไปตามเงื่อนไขและความจำเป็นของผู้ให้บริการหรือหน่วยงานแต่ละแห่งซึ่งในบางกรณีอาจเกิดความไม่สอดคล้องหรือไม่สามารถนำมาใช้งานร่วมกันได้ ดังนั้น จึงได้มีการพัฒนามาตรฐานเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยการดำเนินการที่ผ่านมาสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชนได้ร่วมกันจัดทำมาตรฐานการพิสูจน์และยืนยันตัวตนทางดิจิทัล ได้แก่ ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ (ETDA Recommendation) ซึ่งมีการพัฒนาและปรับปรุงมาอย่างต่อเนื่อง ดังนี้

- เวอร์ชัน 1.0: เลขที่ ขมธอ. 18-2561, 19-2561 และ 20-2561
- เวอร์ชัน 2.0: เลขที่ ขมธอ. 18-2564, 19-2564 และ 20-2564
- เวอร์ชัน 3.0: เลขที่ ขมธอ. 18-2566, 19-2566 และ 20-2566

ในการนี้ เพื่อให้เกิดความสอดคล้องและเสริมสร้างความน่าเชื่อถือและยอมรับในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล และเพื่อให้ผู้ให้บริการและหน่วยงานต่าง ๆ สามารถใช้อ้างอิงและเลือกใช้งานดิจิทัลไอดีร่วมกันได้บนมาตรฐานและระดับความน่าเชื่อถือที่มีความสอดคล้องกัน คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงเห็นควรให้มีการยกระดับมาตรฐานดังกล่าว โดยนำข้อเสนอแนะมาตรฐานฯ เลขที่ ขมธอ. 18-2566, 19-2566 และ 20-2566 มาปรับปรุงเป็นชุดมาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล (เลขที่ มธอ. 11) ซึ่งประกอบด้วย

- เล่ม 1 กรอบการทำงาน (Part 1: Framework)
- เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน (Part 2: Identity Proofing Requirements)
- เล่ม 3 ข้อกำหนดของการยืนยันตัวตน (Part 3: Authentication Requirements)

สำหรับการพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 3 ข้อกำหนดของการยืนยันตัวตน ฉบับนี้ เป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนและการยืนยันตัวตนของผู้ใช้บริการ เพื่อให้ IdP มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกันตามระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL)

สารบัญ

หน้า

1. ขอบข่าย **1**

2. ระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL) **1**

2.1 ระดับ AAL1 1

2.2 ระดับ AAL2 2

2.3 ระดับ AAL3 3

2.4 สรุปข้อกำหนดที่สำคัญของการยืนยันตัวตนตามระดับ AAL 4

3. ข้อกำหนดตามชนิดของสิ่งที่ใช้ยืนยันตัวตน **5**

3.1 รหัสลับจดจำ (memorized secret) 5

3.2 อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device) 6

3.3 อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device) 7

3.4 อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device) 8

3.5 ซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software) 8

3.6 อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic device) 9

3.7 ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic software) 10

3.8 อุปกรณ์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic device) 10

4. ข้อกำหนดทั่วไปของสิ่งที่ใช้ยืนยันตัวตน **11**

4.1 สิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์ (ประเภทสิ่งที่คุณมี) 11

4.2 การจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาด 12

4.3 การใช้งานชีวมิติ (ลงทะเบียนใช้ร่วมกับสิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์เท่านั้น) 12

4.4 การป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance) 13

4.5 การป้องกัน IdP ตัวปลอม (IdP impersonation resistance) 14

5. การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน **14**

5.1 การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน 14

5.2 การสูญหาย ถูกขโมย เสียหาย และการออกทดแทน 15

5.3 การหมดอายุและการออกใหม่ 16

5.4 การเพิกถอน 16

ภาคผนวก ก. อินโฟกราฟิกส์ของระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) **17**

บรรณานุกรม **18**

สารบัญตาราง

หน้า

ตารางที่ 1 สรุปข้อกำหนดที่สำคัญของการยืนยันตัวตนตามระดับ AAL 4

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 3: ข้อกำหนดของการยืนยันตัวตน

1. ขอบข่าย

มาตรฐานฉบับนี้เป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนและการยืนยันตัวตนของผู้ใช้บริการ เพื่อให้ IdP มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกันตามระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL)

มาตรฐานฉบับนี้เป็นข้อกำหนดสำหรับหน่วยงานที่ให้บริการพิสูจน์และยืนยันตัวตนแก่บุคคลภายนอก ข้อกำหนดในมาตรฐานฉบับนี้สามารถประยุกต์ใช้ได้กับบริการพิสูจน์และยืนยันตัวตนที่ใช้เพื่อประโยชน์ภายในกิจการของตนเอง ทั้งนี้ ไม่มีเจตนาปิดกั้นหรือห้ามใช้วิธีการอื่นเพื่อเพิ่มประสิทธิภาพของการพิสูจน์และยืนยันตัวตน

ระดับ AAL ในมาตรฐานฉบับนี้กำหนดชนิดของสิ่งที่ใช้ยืนยันตัวตนและเกณฑ์วิธีการยืนยันตัวตน โดยพิจารณาจากคุณสมบัติในการป้องกันการโจมตีทางไซเบอร์ที่อาจเกิดขึ้นผ่านช่องทางออนไลน์เป็นหลัก เช่น การโจมตีโดยคนกลาง (man-in-the-middle attack) และการโจมตีแบบส่งข้อมูลซ้ำ (replay attack) ด้วยเหตุนี้ การยืนยันตัวตนแบบพบเห็นต่อหน้าซึ่งไม่สามารถนำคุณสมบัติและเกณฑ์การกำหนดระดับ AAL ของการยืนยันตัวตนผ่านช่องทางออนไลน์มาพิจารณาใช้ได้จึงไม่อยู่ในขอบข่ายของมาตรฐานฉบับนี้ ในกรณีที่ IdP มีความประสงค์จะให้บริการยืนยันตัวตนแบบพบเห็นต่อหน้า ให้ใช้วิธีการยืนยันตัวตนที่เหมาะสมตามความต้องการที่ผู้อาศัยการยืนยันตัวตน (relying party: RP) กำหนด

มาตรฐานฉบับนี้มีรูปแบบของคำที่ใช้แสดงออกถึงคุณลักษณะของเนื้อหาเชิงบรรทัดฐาน (normative) และเนื้อหาเชิงให้ข้อมูล (informative) ดังต่อไปนี้

- “ต้อง” (shall) ใช้ระบุสิ่งที่เป็นข้อกำหนด (requirement) ซึ่งต้องปฏิบัติตาม
- “ควร” (should) ใช้ระบุสิ่งที่เป็นข้อแนะนำ (recommendation)
- “อาจ” (may) ใช้ระบุสิ่งที่ยินยอมหรืออนุญาตให้ทำได้ (permission)

2. ระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL)

ระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL) คือ ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของผู้ใช้บริการ โดยระดับ AAL แบ่งออกเป็น 3 ระดับ ดังนี้

2.1 ระดับ AAL1

ระดับ AAL1 ให้ความมั่นใจระดับหนึ่งว่าบุคคลที่กำลังเข้าใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ โดยระดับ AAL1 กำหนดให้ใช้การยืนยันตัวตนแบบปัจจัยเดียว (single-factor authentication) เป็นอย่างน้อย ทั้งนี้ การแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนต้องดำเนินการด้วยเกณฑ์วิธีการยืนยันตัวตน (authentication protocol) ที่มั่นคงปลอดภัย

ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้

การยืนยันตัวตนที่ระดับ AAL1 ต้องใช้ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้

(1) รหัสลับจดจำ (memorized secret)
(2) อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device)
(3) อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device)
(4) ซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software)
(5) อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic device)
(6) สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ที่ระดับ AAL2 และ AAL3

ข้อกำหนดที่สำคัญ

(1) การสื่อสารระหว่างผู้ใช้บริการและ IdP ต้องผ่านช่องทางที่มีความปลอดภัย (authenticated protected channel) เพื่อรักษาความลับของผลลัพธ์ที่ใช้ยืนยันตัวตนและป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance)

2.2 ระดับ AAL2

ระดับ AAL2 ให้ความมั่นใจระดับสูงว่าบุคคลที่กำลังเข้าใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ โดยระดับ AAL2 กำหนดให้ใช้การยืนยันตัวตนด้วยปัจจัยของการยืนยันตัวตน (authentication factor) ที่แตกต่างกัน 2 ปัจจัยเป็นอย่างน้อย ทั้งนี้ การแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมปัจจัยของการยืนยันตัวตนที่แตกต่างกัน 2 ปัจจัยต้องดำเนินการด้วยเกณฑ์วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

หมายเหตุ: การยืนยันตัวตนด้วยปัจจัยของการยืนยันตัวตนที่แตกต่างกัน 2 ปัจจัย สามารถทำได้ 2 วิธี ดังนี้
(1) การใช้สิ่งที่ใช้ยืนยันตัวตนแบบปัจจัยเดียว (single-factor authenticator) ซึ่งเป็นปัจจัยที่แตกต่างกัน จำนวน 2 อัน เช่น การกรอกรหัสผ่าน (สิ่งที่คุณรู้) และข้อมูลลับที่ส่งมายังโทรศัพท์เคลื่อนที่ของผู้ใช้บริการทาง SMS (สิ่งที่คุณมี) เพื่อยืนยันตัวตน
(2) การใช้สิ่งที่ใช้ยืนยันตัวตนแบบหลายปัจจัย (multi-factor authenticator) จำนวน 1 อัน เช่น อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device) ซึ่งจะสร้างรหัสผ่านใช้ครั้งเดียว (OTP) หลังจากผู้ใช้บริการกรอกเลขรหัสส่วนตัวหรือสแกนลายนิ้วมือสำเร็จ จากนั้น ผู้ใช้บริการจะนำ OTP ที่แสดงผลบนอุปกรณ์ไปกรอกเพื่อยืนยันตัวตน

ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้

การยืนยันตัวตนที่ระดับ AAL2 ต้องใช้ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้

(1) อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device)
(2) ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic software)
(3) รหัสลับจดจำ (memorized secret) ร่วมกับ อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device)
(4) รหัสลับจดจำ (memorized secret) ร่วมกับ อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device)
(5) รหัสลับจดจำ (memorized secret) ร่วมกับ ซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software)

(6) สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ที่ระดับ AAL3

ข้อกำหนดที่สำคัญ

(1) การสื่อสารระหว่างผู้ใช้บริการและ IdP ต้องผ่านช่องทางที่มีความปลอดภัย (authenticated protected channel) เพื่อรักษาความลับของผลลัพธ์ที่ใช้ยืนยันตัวตนและป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance)

(2) สิ่งที่ใช้ยืนยันตัวตนอย่างน้อย 1 อันต้องสามารถป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)

(3) เมื่อมีการใช้อุปกรณ์ เช่น โทรศัพท์เคลื่อนที่ ในการยืนยันตัวตน การปลดล็อคอุปกรณ์ดังกล่าว (เช่น การใช้เลขรหัสส่วนตัว (PIN) หรือชีวมิติ) ต้องไม่ถือเป็นหนึ่งในปัจจัยของการยืนยันตัวตน เนื่องจาก IdP จะไม่สามารถทราบได้ว่าอุปกรณ์ถูกล็อคอยู่ หรือกระบวนการปลดล็อคเป็นไปตามข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตนชนิดนั้นหรือไม่

2.3 ระดับ AAL3

ระดับ AAL3 ให้ความมั่นใจระดับสูงมากว่าบุคคลที่กำลังเข้าใช้บริการครอบครองและควบคุมสิ่งที่ใช้ยืนยันตัวตนของผู้ใช้บริการ โดยระดับ AAL3 กำหนดให้ใช้การยืนยันตัวตนด้วยปัจจัยของการยืนยันตัวตนที่แตกต่างกัน 2 ปัจจัยเป็นอย่างน้อย และใช้สิ่งที่ใช้ยืนยันตัวตนที่มีคุณสมบัติเป็นฮาร์ดแวร์ (hardware-based) บรรจุกุญแจเข้ารหัส (cryptographic key) และสามารถป้องกัน IdP ตัวปลอม (IdP impersonation resistance)

ทั้งนี้ การแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมปัจจัยของการยืนยันตัวตนที่แตกต่างกัน 2 ปัจจัยต้องดำเนินการด้วยเกณฑ์วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย รวมถึงการแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมกุญแจเข้ารหัสต้องดำเนินการด้วยเกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol)

ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้

การยืนยันตัวตนที่ระดับ AAL3 ต้องใช้ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้

(1) อุปกรณ์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic device)
(2) อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic device) ร่วมกับ รหัสลับจดจำ (memorized secret)
(3) อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device) ร่วมกับ อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic device)
(4) อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device) เฉพาะที่เป็นฮาร์ดแวร์ ร่วมกับซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software)
(5) อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device) เฉพาะที่เป็นฮาร์ดแวร์ ร่วมกับซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic software)
(6) อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device) เฉพาะที่เป็นฮาร์ดแวร์ ร่วมกับซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software) และรหัสลับจดจำ (memorized secret)

ข้อกำหนดที่สำคัญ

(1) การสื่อสารระหว่างผู้ใช้บริการและ IdP ต้องผ่านช่องทางที่มีความปลอดภัย (authenticated protected channel) เพื่อรักษาความลับของผลลัพธ์ที่ใช้ยืนยันตัวตนและป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance)

(2) สิ่งที่ใช้ยืนยันตัวตนต้องสามารถป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)

(3) สิ่งที่ใช้ยืนยันตัวตนต้องสามารถป้องกัน IdP ตัวปลอม (IdP impersonation resistance)

(4) เมื่อมีการใช้อุปกรณ์ เช่น โทรศัพท์เคลื่อนที่ ในการยืนยันตัวตน การปลดล็อคอุปกรณ์ดังกล่าว (เช่น การใช้เลขรหัสส่วนตัว (PIN) หรือชีวมิติ) ต้องไม่ถือเป็นหนึ่งในปัจจัยของการยืนยันตัวตน เนื่องจาก IdP จะไม่สามารถทราบได้ว่าอุปกรณ์ถูกล็อคอยู่ หรือกระบวนการปลดล็อคเป็นไปตามข้อกำหนดของสิ่งที่ใช้ยืนยันตัวตนชนิดนั้นหรือไม่

2.4 สรุปข้อกำหนดที่สำคัญของการยืนยันตัวตนตามระดับ AAL

ข้อกำหนดที่สำคัญของการยืนยันตัวตนตามระดับ AAL แต่ละระดับสามารถสรุปได้ตามตารางที่ 1

ตารางที่ 1 สรุปข้อกำหนดที่สำคัญของการยืนยันตัวตนตามระดับ AAL

ข้อกำหนดของการยืนยันตัวตน	ระดับ AAL		
	AAL1	AAL2	AAL3
ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้	ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้ (1) memorized secret (2) out-of-band device (3) SF OTP device (4) SF crypto software (5) SF crypto device (6) สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ที่ระดับ AAL2 และ AAL3	ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้ (1) MF OTP device (2) MF crypto software (3) memorized secret + out-of-band device (4) memorized secret + SF OTP device (5) memorized secret + SF crypto software (6) สิ่งที่ใช้ยืนยันตัวตนชนิดอื่น ๆ ที่ระดับ AAL3	ชนิดของสิ่งที่ใช้ยืนยันตัวตนจากตัวเลือกต่อไปนี้ (1) MF crypto device (2) SF crypto device + memorized secret (3) MF OTP device + SF crypto device (4) MF OTP device เฉพาะที่เป็นฮาร์ดแวร์ + SF crypto software (5) SF OTP device เฉพาะที่เป็นฮาร์ดแวร์ + MF crypto software (6) SF OTP device เฉพาะที่เป็นฮาร์ดแวร์ + SF crypto software + memorized secret

ข้อกำหนดของการยืนยันตัวตน	ระดับ AAL		
	AAL1	AAL2	AAL3
การป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance)	✓	✓	✓
การป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)		✓	✓
การป้องกัน IdP ตัวปลอม (IdP impersonation resistance)			✓

หมายเหตุ: SF ย่อมาจาก “single-factor”, MF ย่อมาจาก “multi-factor” และ crypto ย่อมาจาก “cryptographic”

3. ข้อกำหนดตามชนิดของสิ่งที่ใช้ยืนยันตัวตน

ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่ IdP สามารถออกหรือลงทะเบียนให้กับผู้ใช้บริการเพื่อใช้ในการยืนยันตัวตนตามระดับ AAL มีดังนี้

(1) รหัสลับจดจำ (memorized secret)
(2) อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device)
(3) อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device)
(4) อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device)
(5) ซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software)
(6) อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic device)
(7) ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic software)
(8) อุปกรณ์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic device)

3.1 รหัสลับจดจำ (memorized secret)

รหัสลับจดจำ (memorized secret) หรือที่รู้จักกันโดยทั่วไปว่ารหัสผ่าน (password) หรือเลขรหัสส่วนตัว (personal identification number: PIN) เป็นข้อมูลลับที่ให้ผู้ใช้บริการจดจำ ทั้งนี้ รหัสลับจดจำต้องมีความซับซ้อนในระดับที่ยากแก่การคาดเดาโดยผู้ไม่ประสงค์ดี

รหัสลับจดจำเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณรู้ (something you know)

ข้อกำหนดทางเทคนิค

(1) เลขรหัสส่วนตัว (PIN) ที่ลงทะเบียนใช้กับอุปกรณ์ที่เฉพาะเจาะจงต้องมีความยาวของตัวเลขอย่างน้อย 6 หลัก ขณะที่รหัสผ่าน (password) ต้องมีความยาวอย่างน้อย 8 อักขระ

(2) IdP ควรกำหนดรายการรหัสลับจดจำที่ไม่ปลอดภัย (blacklist) เพื่อไม่ให้ผู้ใช้บริการเลือกรหัสลับจดจำจากรายการดังกล่าว เช่น รหัสผ่านที่เคยถูกโจมตีในอดีต คำที่พบในพจนานุกรม ตัวอักษรซ้ำหรือตัวอักษรเรียงลำดับ และคำที่คาดเดาได้โดยง่าย

(3) IdP ควรมีคำแนะนำสำหรับผู้ใช้บริการในการเลือกรหัสลับจดจำที่คาดเดาได้ยาก เช่น ตัวช่วยวัดระดับความปลอดภัยของรหัสผ่าน

(4) IdP ต้องมีการจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามที่กำหนดในหัวข้อ 4.2

3.2 อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device)

อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device) เป็นอุปกรณ์ที่สามารถสื่อสารกับ IdP อย่างปลอดภัยผ่านช่องทางสื่อสารรอง (secondary channel) ซึ่งแยกจากช่องทางสื่อสารหลัก (primary channel) ที่ใช้ในการยืนยันตัวตน

อุปกรณ์สื่อสารช่องทางอื่นเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี (something you have)

อุปกรณ์สื่อสารช่องทางอื่นสามารถทำงานด้วยวิธีการใดวิธีการหนึ่ง ดังนี้

(1) ผู้ใช้บริการได้รับข้อมูลลับจากอุปกรณ์สื่อสารช่องทางอื่นผ่านช่องทางสื่อสารรอง และส่งข้อมูลลับนั้นไปยัง IdP โดยใช้ช่องทางสื่อสารหลัก ตัวอย่างเช่น ผู้ใช้บริการได้รับข้อมูลลับเป็นตัวเลข 6 หลักที่ส่งมายังโทรศัพท์เคลื่อนที่ทาง SMS และกรอกข้อมูลลับนั้นบนหน้าต่างยืนยันตัวตน

(2) ผู้ใช้บริการได้รับข้อมูลลับผ่านช่องทางสื่อสารหลัก และใช้อุปกรณ์สื่อสารช่องทางอื่นเพื่อส่งข้อมูลลับนั้นไปยัง IdP โดยใช้ช่องทางสื่อสารรอง ตัวอย่างเช่น ผู้ใช้บริการเห็นข้อมูลลับที่แสดงเป็น QR code บนหน้าต่างยืนยันตัวตน และใช้โทรศัพท์เคลื่อนที่สแกน QR code นั้นเพื่อให้เกิดการส่งข้อมูลลับไปยัง IdP

ข้อกำหนดทางเทคนิค

(1) อุปกรณ์สื่อสารช่องทางอื่นต้องสร้างช่องทางสื่อสารรองที่แยกจากช่องทางสื่อสารหลักเพื่อใช้รับหรือส่งข้อมูลลับกับ IdP ทั้งนี้ อุปกรณ์ปลายทางที่ใช้สื่อสารกับ IdP ผ่านช่องทางสื่อสารหลักและช่องทางสื่อสารรองอาจเป็นอุปกรณ์เดียวกัน โดยอุปกรณ์ดังกล่าวต้องไม่ทำให้ข้อมูลรั่วไหลจากช่องทางหนึ่งไปยังอีกช่องทางหนึ่งได้โดยไม่ได้รับอนุญาตจากผู้ใช้บริการ

(2) วิธีการที่ไม่สามารถแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมอุปกรณ์ที่เฉพาะเจาะจง เช่น วิธีการที่ใช้ voice-over-IP (VoIP) หรืออีเมล ต้องไม่ถือเป็นวิธีการยืนยันตัวตนด้วยอุปกรณ์สื่อสารช่องทางอื่น

(3) อุปกรณ์สื่อสารช่องทางอื่นต้องมีการยืนยันตัวตนของอุปกรณ์กับ IdP ด้วยวิธีการใดวิธีการหนึ่งดังนี้

(3.1) สร้างช่องทางที่มีความปลอดภัย (authenticated protected channel) กับ IdP โดยใช้กระบวนการเข้ารหัสลับ (cryptography) โดยกุญแจเข้ารหัสต้องถูกเก็บไว้ในที่จัดเก็บที่ปลอดภัย (secure storage) อย่างเหมาะสม เช่น keychain storage, trusted platform module (TPM), trusted execution environment (TEE) หรือ secure element (SE)

(3.2) ยืนยันตัวตนของอุปกรณ์ผ่านโครงข่ายโทรศัพท์สาธารณะ โดยใช้ SIM card หรือวิธีการอื่นที่สามารถระบุอุปกรณ์ได้ วิธีการนี้ต้องถูกใช้เฉพาะกรณีที่ IdP ส่งข้อมูลลับมายังอุปกรณ์สื่อสารช่องทางอื่นผ่านโครงข่ายโทรศัพท์สาธารณะเท่านั้น

(4) การยืนยันตัวตนของผู้ใช้บริการต้องใช้วิธีการใดวิธีการหนึ่ง ดังนี้

(4.1) การส่งข้อมูลลับให้ IdP ทางช่องทางสื่อสารหลัก: IdP ต้องส่งข้อมูลลับที่สร้างขึ้นแบบสุ่มไปยังอุปกรณ์สื่อสารช่องทางอื่น จากนั้น IdP ต้องรอการตอบกลับข้อมูลลับนั้นทางช่องทางสื่อสารหลัก

(4.2) การส่งข้อมูลลับให้ IdP ทางช่องทางสื่อสารรอง: IdP ต้องแสดงข้อมูลลับที่สร้างขึ้นแบบสุ่มให้กับผู้ใช้บริการทางช่องทางสื่อสารหลัก จากนั้น IdP ต้องรอการตอบกลับข้อมูลลับนั้นจากอุปกรณ์สื่อสารช่องทางอื่นของผู้ใช้บริการทางช่องทางสื่อสารรอง

(5) ข้อมูลลับที่สร้างขึ้นแบบสุ่มต้องมีความยาวของตัวเลขอย่างน้อย 6 หลัก

(6) IdP ต้องกำหนดระยะเวลาของการตอบกลับข้อมูลลับจากผู้ใช้บริการให้ไม่เกิน 10 นาที หากเกินระยะเวลาที่กำหนด การยืนยันตัวตนดังกล่าวจะถือว่าเป็นการยืนยันตัวตนที่ไม่ถูกต้อง

(7) IdP ต้องยอมรับการตอบกลับข้อมูลลับจากผู้ใช้บริการเพียงครั้งเดียวในช่วงระยะเวลาที่กำหนดเพื่อป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)

(8) IdP ต้องมีการจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามที่กำหนดในหัวข้อ 4.2

3.3 อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device)

อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device) เป็นฮาร์ดแวร์เฉพาะ หรือซอฟต์แวร์ที่ติดตั้งบนอุปกรณ์ (เช่น โทรศัพท์เคลื่อนที่) สำหรับใช้สร้าง OTP โดยผู้ใช้บริการจะนำ OTP ที่แสดงผลบนอุปกรณ์ไปกรอกบนหน้าต่างยืนยันตัวตนของ IdP เพื่อแสดงให้เห็นว่าตนเองครอบครองและควบคุมอุปกรณ์นั้นจริง

อุปกรณ์ OTP แบบปัจจัยเดียวบรรจุข้อมูล 2 ค่าสำหรับใช้สร้าง OTP คือ (1) กุญแจสมมาตร (symmetric key) ซึ่งจะมีค่าคงที่ตลอดอายุการใช้งานของอุปกรณ์ และ (2) nonce ซึ่งจะเปลี่ยนแปลงค่าทุกครั้งที่อุปกรณ์มีการใช้งานหรือเปลี่ยนแปลงค่าตามเวลาปัจจุบัน

อุปกรณ์ OTP แบบปัจจัยเดียวเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี (something you have)

ข้อกำหนดทางเทคนิค

(1) OTP ต้องมีความยาวของตัวเลขอย่างน้อย 6 หลัก

(2) กรณีที่ค่า nonce ที่ใช้สร้าง OTP เปลี่ยนแปลงค่าตามเวลาปัจจุบัน ค่า nonce ต้องมีการเปลี่ยนแปลงอย่างน้อยทุก 2 นาที และ IdP ต้องยอมรับ OTP ที่สร้างจากค่า nonce ดังกล่าวเพียงครั้งเดียวในช่วงระยะเวลาที่กำหนดเพื่อป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)

(3) IdP ต้องมีการจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามที่กำหนดในหัวข้อ 4.2

3.4 อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device)

อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device) เป็นฮาร์ดแวร์เฉพาะ หรือซอฟต์แวร์ที่ติดตั้งบนอุปกรณ์ (เช่น โทรศัพท์เคลื่อนที่) ซึ่งจะสร้าง OTP หลังจากผู้ใช้บริการยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนที่สอง (เช่น กรอกเลขรหัสส่วนตัว (PIN) หรือสแกนลายนิ้วมือ) สำเร็จ โดยผู้ใช้บริการจะนำ OTP ที่แสดงผลบนอุปกรณ์ไปกรอกบนหน้าต่างยืนยันตัวตนของ IdP เพื่อแสดงให้เห็นว่าตนเองครอบครองและควบคุมอุปกรณ์นั้นจริง

ในทำนองเดียวกันกับอุปกรณ์ OTP แบบปัจจัยเดียว อุปกรณ์ OTP แบบหลายปัจจัยบรรจุข้อมูล 2 ค่า สำหรับใช้สร้าง OTP คือ (1) กุญแจสมมาตร (symmetric key) ซึ่งจะมีค่าคงที่ตลอดอายุการใช้งานของอุปกรณ์ และ (2) nonce ซึ่งจะเปลี่ยนแปลงค่าทุกครั้งที่อุปกรณ์มีการใช้งานหรือเปลี่ยนแปลงค่าตามเวลาปัจจุบัน

อุปกรณ์ OTP แบบหลายปัจจัยเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี (something you have) และจะสร้าง OTP หลังจากผู้ใช้บริการยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนที่สอง ซึ่งเป็นปัจจัยประเภทสิ่งที่คุณรู้ (something you know) หรือสิ่งที่คุณเป็น (something you are)

ข้อกำหนดทางเทคนิค

(1) การยืนยันตัวตนด้วยอุปกรณ์ OTP แบบหลายปัจจัยแต่ละครั้งต้องใช้ปัจจัยของการยืนยันตัวตนทั้ง 2 ปัจจัย

(2) ปัจจัยของการยืนยันตัวตนที่สองต้องเป็นรหัสลับจดจำหรือข้อมูลชีวมิติ

(3) กรณีที่ปัจจัยของการยืนยันตัวตนที่สองเป็นรหัสลับจดจำ รหัสลับจดจำต้องมีความยาวของตัวเลขอย่างน้อย 6 หลัก หรือเป็นไปตามที่กำหนดในหัวข้อ 3.1

(4) กรณีที่ปัจจัยของการยืนยันตัวตนที่สองเป็นข้อมูลชีวมิติ การใช้งานชีวมิติต้องเป็นไปตามที่กำหนดในหัวข้อ 4.3

(5) OTP ต้องมีความยาวของตัวเลขอย่างน้อย 6 หลัก

(6) กรณีที่ค่า nonce ที่ใช้สร้าง OTP เปลี่ยนแปลงค่าตามเวลาปัจจุบัน ค่า nonce ต้องมีการเปลี่ยนแปลงอย่างน้อยทุก 2 นาที และ IdP ต้องยอมรับ OTP ที่สร้างจากค่า nonce ดังกล่าวเพียงครั้งเดียวในช่วงระยะเวลาที่กำหนดเพื่อป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)

(7) IdP ต้องมีการจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามที่กำหนดในหัวข้อ 4.2

3.5 ซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software)

ซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software) เป็นกุญแจเข้ารหัส (cryptographic key) ที่เก็บไว้ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลรูปแบบอื่น

การยืนยันตัวตนด้วยซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียวทำได้โดยการแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมกุญแจเข้ารหัสด้วยเกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol) เช่น

ผู้ใช้บริการลงลายมือชื่อดิจิทัลต่อค่า nonce ที่ส่งมาจาก IdP ด้วยกุญแจเข้ารหัส และส่งผลลัพธ์ให้ IdP ตรวจสอบเพื่อแสดงให้เห็นว่าตนเองครอบครองและควบคุมกุญแจเข้ารหัสนั้นจริง

ซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียวเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี (something you have)

ข้อกำหนดทางเทคนิค

(1) กุญแจเข้ารหัสต้องถูกเก็บไว้ในที่จัดเก็บที่ปลอดภัย (secure storage) อย่างเหมาะสม เช่น keychain storage, trusted platform module (TPM), trusted execution environment (TEE) หรือ secure element (SE)

(2) กุญแจเข้ารหัสต้องถูกปกป้องจากการเปิดเผยโดยไม่ได้รับอนุญาต โดยใช้การควบคุมการเข้าถึง (access control) ซึ่งอนุญาตให้เฉพาะซอฟต์แวร์ที่กำหนดเท่านั้นสามารถเข้าถึงกุญแจเข้ารหัสได้

(3) กุญแจเข้ารหัสและอัลกอริทึมที่ใช้ต้องเป็นไปตามข้อกำหนดขั้นต่ำของมาตรฐาน NIST Special Publication 800-131A Rev. 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths

3.6 อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic device)

อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic device) เป็นอุปกรณ์ที่ใช้กุญแจเข้ารหัส (cryptographic key) ที่ฝังอยู่ภายในอุปกรณ์ เพื่อสร้างผลลัพธ์ที่ใช้ยืนยันตัวตนและส่งผลลัพธ์นั้นไปยังอุปกรณ์ปลายทาง (endpoint) ผ่านการเชื่อมต่อโดยตรง (เช่น ช่องทาง USB port ของคอมพิวเตอร์)

การยืนยันตัวตนด้วยอุปกรณ์เข้ารหัสลับแบบปัจจัยเดียวทำได้โดยการแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมอุปกรณ์เข้ารหัสลับด้วยเกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol) เช่น ผู้ใช้บริการลงลายมือชื่อดิจิทัลต่อค่า nonce ที่ส่งมาจาก IdP ด้วยอุปกรณ์เข้ารหัสลับ และส่งผลลัพธ์ให้ IdP ตรวจสอบเพื่อแสดงให้เห็นว่าตนเองครอบครองและควบคุมอุปกรณ์เข้ารหัสลับนั้นจริง

ข้อแตกต่างระหว่างอุปกรณ์เข้ารหัสลับและซอฟต์แวร์เข้ารหัสลับ คือ ซอฟต์แวร์ที่ฝังอยู่ภายในอุปกรณ์เข้ารหัสลับทั้งหมดจะอยู่ภายใต้การควบคุมดูแลของ IdP หรือผู้ผลิตอุปกรณ์

อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียวเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี (something you have)

ข้อกำหนดทางเทคนิค

(1) กุญแจเข้ารหัสต้องไม่สามารถนำออกจากอุปกรณ์เข้ารหัสลับได้

(2) กุญแจเข้ารหัสต้องถูกปกป้องจากการเปิดเผยโดยไม่ได้รับอนุญาต

(3) อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียวต้องเป็นไปตามมาตรฐาน FIPS 140-2 Security Requirements for Cryptographic Modules ที่ระดับ 1 เป็นอย่างน้อย

(4) กุญแจเข้ารหัสและอัลกอริทึมที่ใช้ต้องเป็นไปตามข้อกำหนดขั้นต่ำของมาตรฐาน NIST Special Publication 800-131A Rev. 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths

3.7 ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic software)

ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic software) เป็นกุญแจเข้ารหัส (cryptographic key) ที่เก็บไว้ในฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลรูปแบบอื่น ซึ่งจะสามารถใช้งานได้หลังจากผู้ใช้บริการยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนที่สอง (เช่น กรอกเลขรหัสส่วนตัว (PIN) หรือสแกนลายนิ้วมือ) สำเร็จ

การยืนยันตัวตนด้วยซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัยทำได้โดยการแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมกุญแจเข้ารหัสด้วยเกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol) เช่น ผู้ใช้บริการลงลายมือชื่อดิจิทัลต่อค่า nonce ที่ส่งมาจาก IdP ด้วยกุญแจเข้ารหัส และส่งผลลัพธ์ให้ IdP ตรวจสอบเพื่อแสดงให้เห็นว่าตนเองครอบครองและควบคุมกุญแจเข้ารหัสนั้นจริง

ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัยเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี (something you have) และจะใช้งานได้หลังจากผู้ใช้บริการยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนที่สอง ซึ่งเป็นปัจจัยประเภทสิ่งที่คุณรู้ (something you know) หรือสิ่งที่คุณเป็น (something you are)

ข้อกำหนดทางเทคนิค

(1) การยืนยันตัวตนด้วยซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัยแต่ละครั้งต้องใช้ปัจจัยของการยืนยันตัวตนทั้ง 2 ปัจจัย

(2) ปัจจัยของการยืนยันตัวตนที่สองต้องเป็นรหัสลับจดจำหรือข้อมูลชีวมิติ

(3) กรณีที่ปัจจัยของการยืนยันตัวตนที่สองเป็นรหัสลับจดจำ รหัสลับจดจำต้องมีความยาวของตัวเลขอย่างน้อย 6 หลัก หรือเป็นไปตามที่กำหนดในหัวข้อ 3.1 และต้องมีการจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามที่กำหนดในหัวข้อ 4.2

(4) กรณีที่ปัจจัยของการยืนยันตัวตนที่สองเป็นข้อมูลชีวมิติ การใช้งานชีวมิติต้องเป็นไปตามที่กำหนดในหัวข้อ 4.3

(5) กุญแจเข้ารหัสควรถูกเก็บไว้ในที่จัดเก็บที่ปลอดภัย (secure storage) อย่างเหมาะสม เช่น keychain storage, trusted platform module (TPM), trusted execution environment (TEE) หรือ secure element (SE)

(6) กุญแจเข้ารหัสต้องถูกปกป้องจากการเปิดเผยโดยไม่ได้รับอนุญาต โดยใช้การควบคุมการเข้าถึง (access control) ซึ่งอนุญาตให้เฉพาะซอฟต์แวร์ที่กำหนดเท่านั้นสามารถเข้าถึงกุญแจเข้ารหัสได้

(7) กุญแจเข้ารหัสและอัลกอริทึมที่ใช้ต้องเป็นไปตามข้อกำหนดขั้นต่ำของมาตรฐาน NIST Special Publication 800-131A Rev. 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths

3.8 อุปกรณ์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic device)

อุปกรณ์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic device) เป็นอุปกรณ์ที่ใช้กุญแจเข้ารหัส (cryptographic key) ที่ฝังอยู่ภายในอุปกรณ์ เพื่อสร้างผลลัพธ์ที่ใช้ยืนยันตัวตนและส่งผลลัพธ์นั้นไปยังอุปกรณ์ปลายทาง (endpoint) ผ่านการเชื่อมต่อโดยตรง (เช่น ช่องทาง USB port ของคอมพิวเตอร์)

ทั้งนี้ กุญแจเข้ารหัสจะสามารถใช้งานได้หลังจากผู้ใช้บริการยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนที่สอง (เช่น กรอกเลขรหัสส่วนตัว (PIN) หรือสแกนลายนิ้วมือ) สำเร็จ

การยืนยันตัวตนด้วยอุปกรณ์เข้ารหัสลับแบบหลายปัจจัยทำได้โดยการแสดงให้เห็นว่าผู้ใช้บริการครอบครองและควบคุมอุปกรณ์เข้ารหัสลับด้วยเกณฑ์วิธีการเข้ารหัสลับ (cryptographic protocol) เช่น ผู้ใช้บริการลงลายมือชื่อดิจิทัลต่อค่า nonce ที่ส่งมาจาก IdP ด้วยอุปกรณ์เข้ารหัสลับ และส่งผลลัพธ์ให้ IdP ตรวจสอบเพื่อแสดงให้เห็นว่าตนเองครอบครองและควบคุมอุปกรณ์เข้ารหัสลับนั้นจริง

ข้อแตกต่างระหว่างอุปกรณ์เข้ารหัสลับและซอฟต์แวร์เข้ารหัสลับ คือ ซอฟต์แวร์ที่ฝังอยู่ภายในอุปกรณ์เข้ารหัสลับทั้งหมดจะอยู่ภายใต้การควบคุมดูแลของ IdP หรือผู้ผลิตอุปกรณ์

อุปกรณ์เข้ารหัสลับแบบหลายปัจจัยเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี (something you have) และจะใช้งานได้หลังจากผู้ใช้บริการยืนยันตัวตนโดยใช้ปัจจัยของการยืนยันตัวตนที่สอง ซึ่งเป็นปัจจัยประเภทสิ่งที่คุณรู้ (something you know) หรือสิ่งที่คุณเป็น (something you are)

ข้อกำหนดทางเทคนิค

(1) การยืนยันตัวตนด้วยอุปกรณ์เข้ารหัสลับแบบหลายปัจจัยแต่ละครั้งต้องใช้ปัจจัยของการยืนยันตัวตนทั้ง 2 ปัจจัย

(2) ปัจจัยของการยืนยันตัวตนที่สองต้องเป็นรหัสลับจดจำหรือข้อมูลชีวมิติ

(3) กรณีที่ปัจจัยของการยืนยันตัวตนที่สองเป็นรหัสลับจดจำ รหัสลับจดจำต้องมีความยาวของตัวเลขอย่างน้อย 6 หลัก หรือเป็นไปตามที่กำหนดในหัวข้อ 3.1 และต้องมีการจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามที่กำหนดในหัวข้อ 4.2

(4) กรณีที่ปัจจัยของการยืนยันตัวตนที่สองเป็นข้อมูลชีวมิติ การใช้งานชีวมิติต้องเป็นไปตามที่กำหนดในหัวข้อ 4.3

(5) กุญแจเข้ารหัสต้องไม่สามารถนำออกจากอุปกรณ์เข้ารหัสลับได้

(6) กุญแจเข้ารหัสต้องถูกปกป้องจากการเปิดเผยโดยไม่ได้รับอนุญาต

(7) อุปกรณ์เข้ารหัสลับแบบหลายปัจจัยต้องเป็นไปตามมาตรฐาน FIPS 140-2 Security Requirements for Cryptographic Modules ที่ระดับ 2 เป็นอย่างน้อย

(8) กุญแจเข้ารหัสและอัลกอริทึมที่ใช้ต้องเป็นไปตามข้อกำหนดขั้นต่ำของมาตรฐาน NIST Special Publication 800-131A Rev. 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths

4. ข้อกำหนดทั่วไปของสิ่งที่ใช้ยืนยันตัวตน

4.1 สิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์ (ประเภทสิ่งที่คุณมี)

IdP ต้องให้คำแนะนำสำหรับผู้ใช้บริการเกี่ยวกับวิธีการป้องกันสิ่งที่ใช้ยืนยันตัวตนจากการสูญหายหรือถูกขโมย และต้องมีกลไกในการเพิกถอนหรือระงับการใช้งานสิ่งที่ใช้ยืนยันตัวตนในทันทีหลังจากได้รับแจ้งจากผู้ใช้บริการว่าสิ่งที่ใช้ยืนยันตัวตนสูญหายหรือถูกขโมย

4.2 การจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาด

กรณีที่สิ่งที่ใช้ยืนยันตัวตนชนิดนั้นกำหนดให้ IdP มีการจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาด IdP ต้องมีกระบวนการป้องกันการโจมตีแบบเดาสุ่ม (online guessing attack) เช่น การเดาสุ่มรหัสลับจดจำ โดย IdP ต้องจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดต่อเนื่องของผู้ใช้บริการแต่ละราย (เช่น ไม่เกิน 100 ครั้ง) หากเกินจำนวนที่กำหนด IdP ควรระงับการยืนยันตัวตนของผู้ใช้บริการดังกล่าว

เพื่อลดโอกาสจากการโจมตีที่จะทำให้ผู้ใช้บริการถูกระงับใช้งานเนื่องจากการยืนยันตัวตนผิดพลาดต่อเนื่องเกินจำนวนที่กำหนด IdP อาจเลือกใช้วิธีการ ดังนี้

(1) กำหนดให้ผู้ใช้บริการต้องผ่านการทดสอบ CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) ก่อนจะยืนยันตัวตน

(2) กำหนดให้ผู้ใช้บริการรอหลังจากยืนยันตัวตนผิดพลาดเป็นระยะเวลาหนึ่ง และจะหน่วงเวลาเพิ่มขึ้นทุกครั้งที่ผู้ใช้บริการยืนยันตัวตนผิดพลาดต่อเนื่องกัน (เช่น เพิ่มขึ้นจาก 30 วินาทีไปจนถึง 1 ชั่วโมงตามจำนวนครั้งของการยืนยันตัวตนผิดพลาด)

(3) ยอมรับเฉพาะการยืนยันตัวตนที่มาจาก IP address ซึ่งผู้ใช้บริการเคยยืนยันตัวตนสำเร็จมาก่อนเท่านั้น

เมื่อผู้ใช้บริการยืนยันตัวตนสำเร็จ IdP ควรมองข้ามการยืนยันตัวตนผิดพลาดครั้งก่อนหน้าของผู้ใช้บริการดังกล่าวที่มาจาก IP address เดียวกัน

4.3 การใช้งานชีวมิติ (ลงทะเบียนใช้ร่วมกับสิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์เท่านั้น)

การใช้งานชีวมิติ (biometrics) เช่น ภาพใบหน้า ลายนิ้วมือ และลายม่านตา ในการยืนยันตัวตน ถือเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณเป็น (something you are) ทั้งนี้ สิ่งที่ใช้ยืนยันตัวตนที่สามารถรองรับการใช้งานชีวมิติสำหรับการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) ประกอบด้วย อุปกรณ์ OTP แบบหลายปัจจัย ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย และอุปกรณ์เข้ารหัสลับแบบหลายปัจจัย

การใช้งานชีวมิติในการยืนยันตัวตนยังมีข้อจำกัดเนื่องจากเหตุผล ดังนี้ [1]

(1) การใช้งานชีวมิติมีอัตราการเข้าคู่ผิดพลาด (false match rate: FMR) ซึ่งทำให้เกิดความไม่มั่นใจว่าผู้ที่กำลังยืนยันตัวตนคือผู้ใช้บริการตัวจริง และอาจถูกโจมตีด้วยการใช้ภาพใบหน้าหรือลายนิ้วมือปลอม (spoofing attack)

(2) การเปรียบเทียบข้อมูลชีวมิติ (biometric comparision) เป็นการเปรียบเทียบบนพื้นฐานของความน่าจะเป็น (probabilistic) ขณะที่ปัจจัยของการยืนยันตัวตนประเภทอื่น ๆ เป็นการเปรียบเทียบอย่างชัดเจนว่าข้อมูลตรงกันหรือไม่ (deterministic)

(3) วิธีการเพิกถอนข้อมูลชีวมิติ ยังมีข้อจำกัดเกี่ยวกับความพร้อมใช้งานและมาตรฐานการทดสอบ

(4) ชีวมิติไม่ถือเป็นข้อมูลลับ เนื่องจากผู้ไม่ประสงค์ดีสามารถขโมยชีวมิติของบุคคลจากการค้นหาข้อมูลทางออนไลน์หรือการถ่ายภาพบุคคลด้วยกล้องโทรศัพท์ (กรณีที่เป็นใบหน้า) การล่อลวงให้บุคคลใช้มือสัมผัสวัตถุ (กรณีที่เป็นลายนิ้วมือ) หรือการถ่ายภาพความละเอียดสูง

(กรณีที่เป็นม่านตา)

ด้วยเหตุนี้ การใช้งานชีวมิติในการยืนยันตัวตนมีข้อกำหนด ดังนี้

(1) ชีวมิติต้องใช้เป็นปัจจัยร่วมของการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) และลงทะเบียนใช้ร่วมกับสิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์ (ประเภทสิ่งที่คุณมี) เท่านั้น เนื่องจากหากตรวจพบว่าผู้ใช้บริการเป็นตัวปลอมหรือสงสัยว่ามีการใช้งานในทางที่ผิด IdP สามารถเพิกถอนสิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์นั้น ทดแทนการเพิกถอนข้อมูลชีวมิติ ซึ่งมีข้อจำกัด

(2) การเปรียบเทียบข้อมูลชีวมิติสามารถดำเนินการที่อุปกรณ์ของผู้ใช้บริการหรือที่ระบบงานของ IdP ทั้งนี้ หากการเปรียบเทียบข้อมูลชีวมิติดำเนินการที่ระบบงานของ IdP การรับส่งข้อมูลชีวมิติระหว่างอุปกรณ์รับข้อมูล (sensor) กับ IdP ต้องดำเนินการผ่านช่องทางที่มีความปลอดภัย (authenticated protected channel)

(3) ความแม่นยำในการเปรียบเทียบข้อมูลชีวมิติต้องมีอัตราการเข้าคู่ผิดพลาด (false match rate: FMR) ไม่เกิน 0.01% และอัตราการไม่เข้าคู่ผิดพลาด (false non-match rate: FNMR) ไม่เกิน 3% [2]

(4) IdP ต้องมีเทคโนโลยีการตรวจจับการปลอมแปลงชีวมิติ (presentation attack detection) เช่น การตรวจจับการมีชีวิตของบุคคล (liveness detection) เพื่อช่วยป้องกันการโจมตีด้วยการใช้ภาพใบหน้าหรือลายนิ้วมือปลอม (spoofing attack) ทั้งนี้ IdP สามารถพิจารณาการทดสอบความสามารถของเทคโนโลยีการตรวจจับการปลอมแปลงชีวมิติให้สอดคล้องหรือเทียบเคียงได้ตามมาตรฐานสากล เช่น ISO/IEC 30107 Information technology – Biometric presentation attack detection หรือ FIDO Biometrics Requirements

(5) IdP อาจจำกัดจำนวนครั้งของการยืนยันตัวตนด้วยชีวมิติที่ผิดพลาดต่อเนื่อง (เช่น ไม่เกิน 10 ครั้ง) หากเกินจำนวนที่กำหนด IdP อาจเลือกใช้วิธีการ ดังนี้

(5.1) หน่วงเวลาเป็นระยะเวลาหนึ่งก่อนจะให้ยืนยันตัวตนครั้งต่อไป และจะหน่วงเวลาเพิ่มขึ้นทุกครั้งที่ผู้ใช้บริการยืนยันตัวตนผิดพลาดต่อเนื่องกัน (เช่น เพิ่มขึ้นจาก 30 วินาทีไปจนถึง 1 ชั่วโมงตามจำนวนครั้งของการยืนยันตัวตนผิดพลาด)

(5.2) ระงับการยืนยันตัวตนด้วยชีวมิติของผู้ใช้บริการ และเสนอให้ผู้ใช้บริการยืนยันตัวตนด้วยสิ่งที่ใช้ยืนยันตัวตนชนิดอื่น (ถ้ามี)

4.4 การป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)

กระบวนการยืนยันตัวตนสามารถป้องกันการโจมตีแบบส่งข้อมูลซ้ำได้ หากการบันทึกและนำผลลัพธ์ที่ใช้ยืนยันตัวตนครั้งก่อนหน้ามาส่งซ้ำไม่สามารถทำให้การยืนยันตัวตนสำเร็จ ทั้งนี้ การป้องกันการโจมตีแบบส่งข้อมูลซ้ำเป็นการดำเนินการเพิ่มเติมจากการสื่อสารผ่านช่องทางที่มีความปลอดภัย (authenticated protected channel) เนื่องจากผลลัพธ์ที่ใช้ยืนยันตัวตนอาจถูกขโมยโดยผู้ไม่ประสงค์ดีก่อนที่จะส่งเข้าสู่ช่องทางที่มีความปลอดภัย

สิ่งที่ใช้ยืนยันตัวตนที่ใช้ค่า nonce เพื่อพิสูจน์ความใหม่ (freshness) ของผลลัพธ์ที่ใช้ยืนยันตัวตน จะมีคุณสมบัติในการป้องกันการโจมตีแบบส่งข้อมูลซ้ำ เนื่องจาก IdP สามารถตรวจพบได้ทันทีว่าผลลัพธ์ซึ่งไม่มีค่า nonce ที่เหมาะสม คือ ผลลัพธ์ที่ใช้ยืนยันตัวตนครั้งก่อนหน้าซึ่งถูกนำมาส่งซ้ำ

สิ่งที่ใช้ยืนยันตัวตนที่มีคุณสมบัติในการป้องกันการโจมตีแบบส่งข้อมูลซ้ำ ประกอบด้วย อุปกรณ์สื่อสารช่องทางอื่น อุปกรณ์ OTP ซอฟต์แวร์เข้ารหัสลับ และอุปกรณ์เข้ารหัสลับ ขณะที่รหัสลับจดจำไม่มีคุณสมบัติในการป้องกันการโจมตีแบบส่งข้อมูลซ้ำ เนื่องจากรหัสลับจดจำถูกนำมาใช้ซ้ำสำหรับการยืนยันตัวตนแต่ละครั้ง

4.5 การป้องกัน IdP ตัวปลอม (IdP impersonation resistance)

การโจมตีด้วยการปลอมตัวเป็น IdP หรือที่รู้จักกันว่า การโจมตีแบบฟิชชิง (phishing attack) เป็นการหลอกลวงให้ผู้ใช้บริการหลงเชื่อเข้ามายืนยันตัวตนบนเว็บไซต์ของ IdP ตัวปลอม

กระบวนการยืนยันตัวตนที่ป้องกัน IdP ตัวปลอม<u>ต้อง</u>สร้างช่องทางที่มีความปลอดภัย (authenticated protected channel) กับ IdP และ<u>ต้อง</u>เชื่อมโยงตัวระบุช่องทาง (channel identifier) ของช่องทางที่มีความปลอดภัยนั้นกับผลลัพธ์ที่ใช้ยืนยันตัวตน ด้วยการใช้กุญแจส่วนตัว (private key) ของผู้ใช้บริการลงลายมือชื่อดิจิทัลกับข้อมูลทั้งสองค่า จากนั้น IdP <u>ต้อง</u>ตรวจสอบลายมือชื่อดิจิทัลด้วยกุญแจสาธารณะ (public key) ที่สัมพันธ์กันเพื่อยืนยันตัวตนของผู้ใช้บริการ ดังนั้น IdP ตัวปลอมจะไม่สามารถนำลายมือชื่อดิจิทัลไปส่งต่อเพื่อยืนยันตัวตนกับ IdP ตัวจริงได้ เนื่องจากช่องทางดังกล่าวมีตัวระบุช่องทางที่แตกต่างกัน

สิ่งที่ใช้ยืนยันตัวตนที่ไม่มีคุณสมบัติในการป้องกัน IdP ตัวปลอม ประกอบด้วย รหัสลับจดจำ อุปกรณ์สื่อสารช่องทางอื่น และอุปกรณ์ OTP เนื่องจากเป็นสิ่งที่ใช้ยืนยันตัวตนที่ให้ผู้ใช้บริการกรอกผลลัพธ์ที่ใช้ยืนยันตัวตนกับ IdP ด้วยตนเอง ซึ่งการกรอกผลลัพธ์ที่ใช้ยืนยันตัวตนด้วยผู้ใช้บริการจะไม่มีการเชื่อมโยงผลลัพธ์นั้นกับเซสชัน (session) ที่กำลังยืนยันตัวตนอยู่ ทำให้ IdP ตัวปลอมสามารถนำผลลัพธ์ที่ได้มานั้นไปส่งต่อให้กับ IdP ตัวจริงและยืนยันตัวตนเป็นผู้ใช้บริการได้สำเร็จ

5. การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน

IdP ทำหน้าที่เชื่อมโยงอัตลักษณ์ของผู้ใช้บริการเข้ากับสิ่งที่ใช้ยืนยันตัวตนและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนนั้น การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนประกอบด้วยกระบวนการต่าง ๆ ซึ่งขึ้นอยู่กับชนิดของสิ่งที่ใช้ยืนยันตัวตน ดังนี้

(1) การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน
(2) การสูญหาย ถูกขโมย เสียหาย และการออกทดแทน
(3) การหมดอายุและการออกใหม่
(4) การเพิกถอน

5.1 การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน

การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน (authenticator binding) คือ การสร้างความเชื่อมโยงระหว่างสิ่งที่ใช้ยืนยันตัวตนกับบัญชีของผู้ใช้บริการ เพื่อให้สิ่งที่ใช้ยืนยันตัวตนสามารถใช้ยืนยันบัญชีของผู้ใช้บริการนั้นได้ ทั้งนี้ IdP สามารถเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนเข้ากับบัญชีของผู้ใช้บริการโดยการออกสิ่งที่ใช้ยืนยันตัวตนอันใหม่ให้กับผู้ใช้บริการหรือการลงทะเบียนสิ่งที่ใช้ยืนยันตัวตนที่ผู้ใช้บริการมีอยู่ก่อนแล้ว

ข้อกำหนดของการเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน

(1) IdP ต้องเก็บรักษาข้อมูลของสิ่งที่ใช้ยืนยันตัวตนทั้งหมดที่เกี่ยวข้องกับอัตลักษณ์ของผู้ใช้บริการตลอดอายุการใช้งานของดิจิทัลไอดี

(2) ข้อมูลที่เก็บรักษาต้องประกอบด้วยวันที่และเวลาที่เชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนเข้ากับบัญชีของผู้ใช้บริการ และควรประกอบด้วยข้อมูลเกี่ยวกับอุปกรณ์ที่ใช้เชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน เช่น IP address หรือหมายเลขประจำอุปกรณ์

(3) IdP ต้องเก็บรักษาข้อมูลที่จำเป็นสำหรับการจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาดตามที่กำหนดในหัวข้อ 4.2

(4) IdP ต้องตรวจสอบชนิดของสิ่งที่ใช้ยืนยันตัวตนว่าเป็นไปตามข้อกำหนดที่ระดับ AAL แต่ละระดับ

(5) กรณีที่ IdP อนุญาตให้มีการเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนเพิ่มเติมหรือสิ่งที่ใช้ยืนยันตัวตนที่ผู้ใช้บริการมีอยู่ก่อนแล้วเข้ากับบัญชีของผู้ใช้บริการ IdP ต้องให้ผู้ใช้บริการยืนยันตัวตนที่ระดับ AAL ปัจจุบัน (หรือระดับ AAL ที่สูงกว่า) ก่อนที่จะเพิ่มสิ่งที่ใช้ยืนยันตัวตนอันใหม่

(6) เมื่อเพิ่มสิ่งที่ใช้ยืนยันตัวตนอันใหม่แล้ว IdP ควรส่งการแจ้งเตือนให้ผู้ใช้บริการผ่านช่องทางที่เป็นอิสระจากช่องทางที่ใช้เชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนดังกล่าว (เช่น การส่งให้ทางอีเมลของผู้ใช้บริการ)

5.2 การสูญหาย ถูกขโมย เสียหาย และการออกทดแทน

สิ่งที่ใช้ยืนยันตัวตนที่สูญหาย ถูกขโมย หรือเสียหาย ถือว่าเป็นสิ่งที่ใช้ยืนยันตัวตนที่อาจถูกสวมรอยโดยผู้ไม่ประสงค์ดี ดังนั้น IdP ควรมีแนวปฏิบัติที่เหมาะสมในกรณีสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกขโมย และเสียหาย รวมถึงการออกสิ่งที่ใช้ยืนยันตัวตนทดแทนอันเดิม (replacement)

ข้อกำหนดของการสูญหาย ถูกขโมย และเสียหาย

(1) IdP ควรระงับการใช้งาน เพิกถอน หรือยุติการใช้งานสิ่งที่ใช้ยืนยันตัวตน ในทันทีหลังจากตรวจพบว่าสิ่งที่ใช้ยืนยันตัวตนสูญหาย ถูกขโมย หรือเสียหาย

(2) IdP ควรให้ผู้ใช้บริการยืนยันตัวตนด้วยสิ่งที่ใช้ยืนยันตัวตนสำรองหรือวิธีการอื่น ๆ ก่อนจะอนุญาตให้แจ้งการสูญหาย ถูกขโมย และเสียหายของสิ่งที่ใช้ยืนยันตัวตน เพื่อให้มั่นใจว่าการแจ้งเรื่องดังกล่าวมาจากผู้ใช้บริการตัวจริง

(3) สิ่งที่ใช้ยืนยันตัวตนสำรองต้องเป็นรหัสลับจดจำหรือสิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์

ข้อกำหนดของการออกทดแทน

(1) หากสิ่งที่ใช้ยืนยันตัวตนทั้งหมดสูญหาย ถูกขโมย หรือเสียหาย IdP ต้องดำเนินการพิสูจน์ตัวตนของผู้ใช้บริการใหม่ด้วยวิธีการทั้งหมด อย่างไรก็ตาม IdP อาจเลือกใช้การพิสูจน์ตัวตนใหม่ด้วยวิธีการเพียงบางส่วน โดยใช้การตรวจสอบความเชื่อมโยงระหว่างผู้ใช้บริการกับหลักฐานแสดงตนที่ผู้ใช้บริการเคยให้ไว้กับ IdP ในการพิสูจน์ตัวตนครั้งก่อนหน้า

(2) เมื่อออกสิ่งที่ใช้ยืนยันตัวตนทดแทนอันเดิมแล้ว IdP ควรส่งการแจ้งเตือนให้ผู้ใช้บริการทราบ

5.3 การหมดอายุและการออกใหม่

IdP อาจออกสิ่งที่ใช้ยืนยันตัวตนที่กำหนดอายุการใช้งานให้กับผู้ใช้บริการ โดยสิ่งที่ใช้ยืนยันตัวตนที่หมดอายุจะไม่สามารถใช้ในการยืนยันตัวตนได้ ดังนั้น IdP ควรมีแนวปฏิบัติที่เหมาะสมในกรณีสิ่งที่ใช้ยืนยันตัวตนหมดอายุ รวมถึงการออกสิ่งที่ใช้ยืนยันตัวตนอันใหม่ (renewal)

ข้อกำหนดของการหมดอายุ

(1) สิ่งที่ใช้ยืนยันตัวตนที่หมดอายุต้องไม่สามารถใช้ยืนยันตัวตนได้

(2) เมื่อมีการยืนยันตัวตนโดยใช้สิ่งที่ใช้ยืนยันตัวตนที่หมดอายุ IdP ควรแจ้งให้ผู้ใช้บริการทราบว่าการยืนยันตัวตนผิดพลาดเนื่องจากสิ่งที่ใช้ยืนยันตัวตนหมดอายุ

ข้อกำหนดของการออกใหม่

(1) IdP ควรเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนอันใหม่ ในระยะเวลาที่เหมาะสมก่อนที่สิ่งที่ใช้ยืนยันตัวตนอันเดิมจะหมดอายุ

(2) เมื่อผู้ใช้บริการใช้สิ่งที่ใช้ยืนยันตัวตนอันใหม่ได้แล้ว IdP อาจเพิกถอนสิ่งที่ใช้ยืนยันตัวตนอันเดิมในทันที

5.4 การเพิกถอน

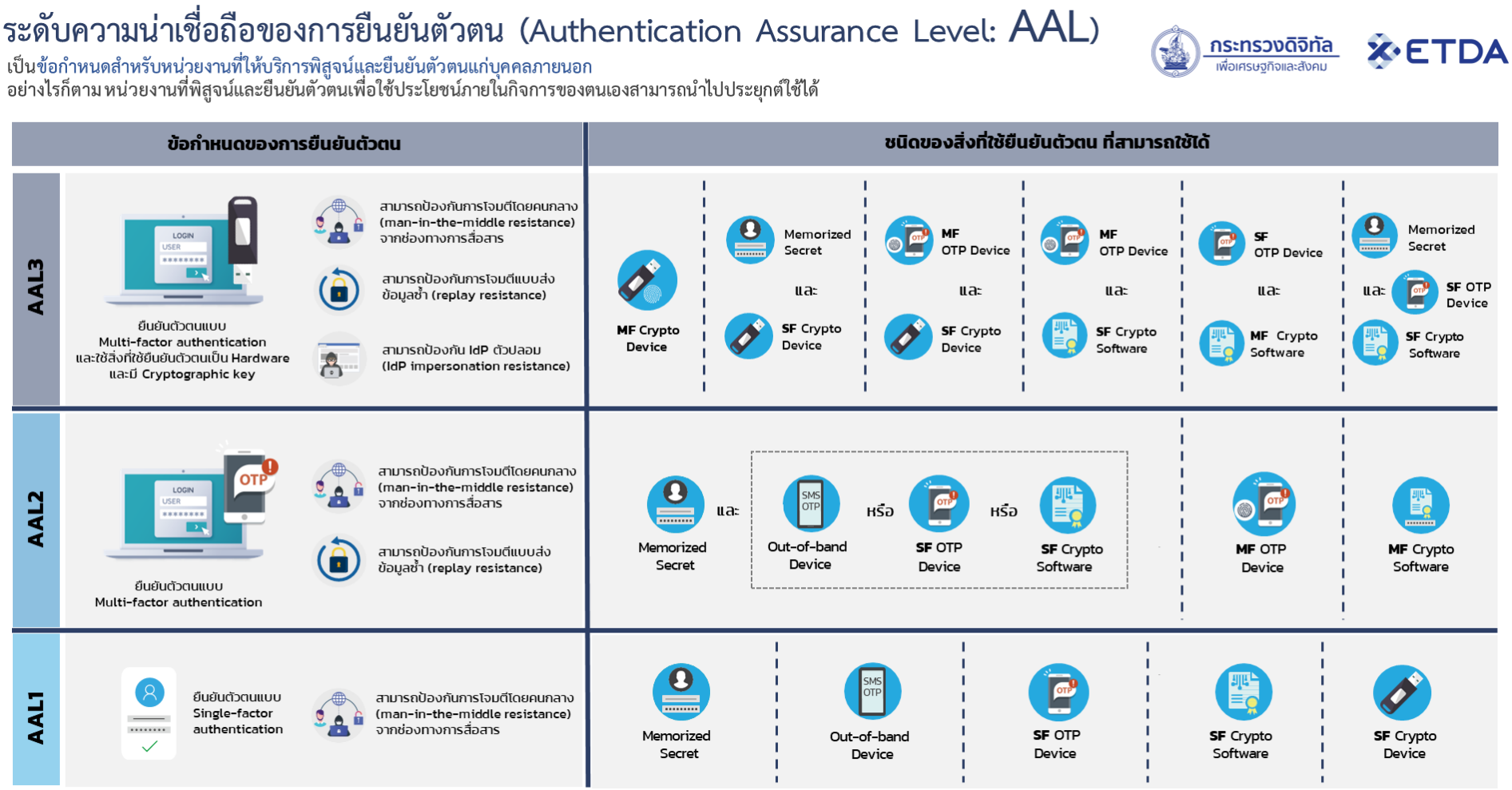
การเพิกถอน (revocation) หรือการยุติการใช้งาน (termination) ของสิ่งที่ใช้ยืนยันตัวตน คือ การลบความเชื่อมโยงระหว่างสิ่งที่ใช้ยืนยันตัวตนกับบัญชีของผู้ใช้บริการ

ข้อกำหนดของการเพิกถอน

(1) IdP ต้องเพิกถอนสิ่งที่ใช้ยืนยันตัวตนในทันที เมื่อทราบกรณี ดังนี้
   (1.1) เมื่อดิจิทัลไอดีหรือบัญชีของผู้ใช้บริการสิ้นสุดลง เช่น การเสียชีวิตของผู้ใช้บริการ หรือการตรวจพบว่าผู้ใช้บริการเป็นตัวปลอม
   (1.2) เมื่อผู้ใช้บริการร้องขอให้เพิกถอนสิ่งที่ใช้ยืนยันตัวตน
   (1.3) เมื่อ IdP พิจารณาว่าผู้ใช้บริการมีคุณสมบัติไม่ตรงตามเกณฑ์ที่กำหนด

ภาคผนวก ก. อินโฟกราฟิกส์ของระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL)

อินโฟกราฟิกส์ (infographics) ของระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level: AAL) ซึ่งเป็นการสรุปข้อกำหนดที่สำคัญบางส่วนจากมาตรฐานเพื่อนำเสนอข้อมูลเป็นภาพที่สามารถเข้าใจได้ง่าย แสดงตามนี้



หมายเหตุ: เป็นการสรุปข้อกำหนดที่สำคัญบางส่วนจากมาตรฐาน

ศึกษารายละเอียดจาก มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 3 ข้อกำหนดของการยืนยันตัวตน (เลขที่ มธอ. 11 เล่ม 3-2566)

บรรณานุกรม

[1] National Institute of Standards and Technology, U.S. Department of Commerce, "NIST Special Publication 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management", June 2017.

[2] Digital Transformation Agency, Australian Government, "Trusted Digital Identity Framework (TDIF): 05 - Role Requirements", Release 4.7, June 2022.

[3] National Institute of Standards and Technology, U.S. Department of Commerce, "NIST Special Publication 800-131A Revision 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths", March 2019.

[4] National Institute of Standards and Technology, U.S. Department of Commerce, "FIPS 140-2, Security Requirements for Cryptographic Modules", May 2001.

[5] International Organization for Standardization, "ISO/IEC 30107-3:2017 Information technology – Biometric presentation attack detection – Part 3: Testing and reporting", September 2017.