คธอ./CDV

กุมภาพันธ์ 2564

ห้ามใช้หรือยึดร่างนี้เป็นมาตรฐาน
มาตรฐานฉบับสมบูรณ์จะมีประกาศโดยคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ร่าง

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 1: กรอบการทำงาน

DIGITAL IDENTITY – PART 1: FRAMEWORK

สำหรับเวียนขอข้อคิดเห็นจากหน่วยงานต่าง ๆ ที่เกี่ยวข้อง

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

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

ELECTRONIC TRANSACTION STANDARD

มธอ. XX-XXXX

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 1: กรอบการทำงาน

DIGITAL IDENTITY –
PART 1: FRAMEWORK

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ICS 35.030

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 1: กรอบการทำงาน

มธอ. XX-XXXX

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

นางอัจฉรินทร์ พัฒนพันธ์ชัย สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

กรรมการผู้ทรงคุณวุฒิ

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

กรรมการและเลขานุการ

นายชัยชนะ มิตรพันธ์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คณะอนุกรรมการมาตรฐานและการกำกับดูแล
ภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

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 กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ
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

คณะทำงานนำร่องการใช้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

(จัดทำข้อเสนอแนะมาตรฐานฯ เลขที่ ขมธอ. 18-2561 ขมธอ. 19-2561 และ ขมธอ. 20-2561)

ประธานคณะทำงานร่วม

นางสาวสิริธิดา พนมวัน ณ อยุธยา	ธนาคารแห่งประเทศไทย
นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

รองประธานคณะทำงาน

นายอาศิส อัญญะโพธิ์	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

คณะทำงาน

นายอภิวัฒน์ อินขัด	กรมการกงสุล
นายวีนัส สีสุข	กรมการปกครอง
นายสัญชัย เตชนิมิตวัช	
นายสุชาติ ธานีรัตน์	
นายเผด็จ เรือนจันทร์	กรมพัฒนาธุรกิจการค้า
นางสาวขนิษฐา สหเมธาพัฒน์	กรมสรรพากร
นางอารีย์พันธ์ เจริญสุข	สำนักงานคณะกรรมการพัฒนาระบบราชการ
นางสาวนิชา สาทรกิจ	
นางวณิสรา สุขวัฒน์	
นายสุวิจักขณ์ ธรรมชัยพจน์	สำนักงานป้องกันและปราบปรามการฟอกเงิน
นายสรรเพชญ แสงเนตรสว่าง	
นายบัญชา มนูญกุลชัย	ธนาคารแห่งประเทศไทย
นายสุวิทย์ ตันรุ่งเรือง	
นางสาวสาริกา อภิวรรธกกุล	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
นายศุภกิจ สัตยารัฐ	สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
นายอนุชิต ชื่นชมภู	บริษัท ไปรษณีย์ไทย จำกัด
นายณัฐ เลิศฤทธิ์	
นางสาวนันทวัน วงศ์ขจรกิตติ	กองทุนเงินให้กู้ยืมเพื่อการศึกษา
นางวรวรรณ ธาราภูมิ	สมาคมบริษัทจัดการลงทุน
นางสาวยุภาวรรณ ศิริชัยนฤมิตร	ตลาดหลักทรัพย์แห่งประเทศไทย
นายฐานิสร์ ฟอลเล็ต	สมาคมการค้าผู้ให้บริการชำระเงินอิเล็กทรอนิกส์ไทย
นายฐากร ปิยะพันธ์	สมาคมธนาคารไทย
นางสาวสุญาณี ภูริปัญญวานิช	สมาคมธนาคารไทย
นายสุวิชชา สุดใจ	สมาคมธนาคารไทย
นายศีลวัต สันติวิสัฏฐ์	สมาคมธนาคารไทย
นางอภิพันธ์ เจริญอนุสรณ์	สมาคมธนาคารไทย

นางประราลี รัตน์ประสาทพร	สมาคมธนาคารไทย
นางภัทธีรา ดิลกรุ่งธีระภพ	สมาคมบริษัทหลักทรัพย์ไทย
นายพิเชษฐ สิทธิอำนวย	สมาคมบริษัทหลักทรัพย์ไทย
นายญาณศักดิ์ มโนมัยพิบูลย์	สมาคมบริษัทหลักทรัพย์ไทย
นายสุรศักดิ์ กลิ่นศรีสุข	สมาคมประกันชีวิตไทย
นายจรุง เชื้อจินดา	สมาคมประกันชีวิตไทย
นายพีระพัฒน์ เมฆสิงห์วี	สมาคมประกันวินาศภัยไทย
นายชูชัย วชิรบรรจง	สมาคมประกันวินาศภัยไทย

คณะทำงานและเลขานุการร่วม

นายศุภโชค จันทรประทิน	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
นายธนฉัตร วิจารณ์ปรีชา	ธนาคารเกียรตินาคิน จำกัด (มหาชน)

ผู้ช่วยเลขานุการ

นายนครินทร์ ลิ้มรังษี	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

คำนำ

การพิสูจน์และยืนยันตัวตนของบุคคลเป็นขั้นตอนสำคัญในการทำธุรกรรมในระบบเศรษฐกิจ แต่ที่ผ่านมาผู้ที่ประสงค์จะขอรับบริการจากผู้ประกอบการหรือหน่วยงานใด ๆ จะต้องทำการพิสูจน์และยืนยันตัวตนโดยการแสดงตนต่อผู้ให้บริการพร้อมกับต้องส่งเอกสารหลักฐาน ซึ่งเป็นภาระต่อผู้ใช้บริการและผู้ให้บริการ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชนจึงได้ร่วมกันจัดทำมาตรฐานแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย โดยประกาศเป็นข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ (ETDA Recommendation) เมื่อวันที่ 28 กันยายน พ.ศ. 2561 ซึ่งประกอบด้วยข้อเสนอแนะมาตรฐานฯ จำนวน 3 ฉบับ ดังนี้

(1) ข้อเสนอแนะมาตรฐานฯ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ (เวอร์ชัน 1.0) เลขที่ ขมธอ. 18-2561
(2) ข้อเสนอแนะมาตรฐานฯ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน (เวอร์ชัน 1.0) เลขที่ ขมธอ. 19-2561
(3) ข้อเสนอแนะมาตรฐานฯ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน (เวอร์ชัน 1.0) เลขที่ ขมธอ. 20-2561

ต่อมา กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์กำหนดให้บุคคลสามารถพิสูจน์และยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ โดยมีกลไกการควบคุมดูแลผู้ประกอบธุรกิจบริการที่เกี่ยวข้องเพื่อให้ระบบดังกล่าวมีความน่าเชื่อถือและปลอดภัย ป้องกันความเสียหายที่อาจเกิดขึ้นต่อสาธารณชน ตลอดจนเสริมสร้างความน่าเชื่อถือและการยอมรับในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ได้พิจารณาแก้ไขปรับปรุงข้อเสนอแนะมาตรฐานฯ ฉบับเดิม เพื่อให้แนวทางการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความสอดคล้องกับบริบทการใช้งาน ความต้องการทางธุรกิจ และคุณลักษณะของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลในประเทศไทย โดยกำหนดเป็นมาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อมาใช้แทนข้อเสนอแนะมาตรฐานฯ ฉบับเดิม และยกเลิกข้อเสนอแนะมาตรฐานฯ ฉบับเดิม (ข้อเสนอแนะมาตรฐานฯ เลขที่ ขมธอ. 18-2561 ขมธอ. 19-2561 และ ขมธอ. 20-2561)

มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล ประกอบด้วยมาตรฐานจำนวน 3 ฉบับ ดังนี้

(1) มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 1 กรอบการทำงาน (Digital Identity – Part 1: Framework)
(2) มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน (Digital Identity – Part 2: Identity Proofing Requirements)
(3) มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 3 ข้อกำหนดของการยืนยันตัวตน (Digital Identity – Part 3: Authentication Requirements)

การพิสูจน์และยืนยันตัวตนทางดิจิทัล – 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 **6**

4.1 ภาพรวม 6

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 คุณลักษณะ (identity attribute) หมายถึง ข้อมูลที่เกี่ยวข้องกับบุคคล ตัวอย่างเช่น เลขประจำตัว ชื่อบุคคล วันเดือนปีเกิด ที่อยู่อีเมล หมายเลขโทรศัพท์เคลื่อนที่ หรือข้อมูลระบุอุปกรณ์ที่บุคคลใช้งาน

2.3 อัตลักษณ์ (identity) หมายถึง คุณลักษณะหรือชุดของคุณลักษณะที่เกี่ยวข้องกับตัวบุคคล ซึ่งเป็นลักษณะเฉพาะและสามารถบ่งบอกหรือจำแนกบุคคลได้ภายในบริบทที่กำหนด [2]

2.4 หลักฐานแสดงตน (identity evidence หรือ identity document) หมายถึง เอกสารทางกายภาพหรือข้อมูลอิเล็กทรอนิกส์ ซึ่งสามารถใช้เป็นหลักฐานในการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคล

2.5 สิ่งที่ใช้ยืนยันตัวตน (authenticator) หมายถึง สิ่งที่บุคคลเป็นเจ้าของหรือครอบครองเพื่อใช้ในการยืนยันอัตลักษณ์ของบุคคล โดยสิ่งที่ใช้ยืนยันตัวตนทุกอันจะมีปัจจัยของการยืนยันตัวตน (authentication factor) อย่างน้อยหนึ่งปัจจัย ได้แก่ สิ่งที่คุณรู้ (something you know) สิ่งที่คุณมี (something you have) และสิ่งที่คุณเป็น (something you are)

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

2.7 การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน (authenticator management) หมายถึง กระบวนการเชื่อมโยงอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้ยืนยันตัวตน และการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนนั้น [2]

2.8 การยืนยันตัวตน (authentication) หมายถึง กระบวนการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน เพื่อยืนยันอัตลักษณ์ของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตนนั้น [2]

2.9 ผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) หมายถึง หน่วยงานที่ให้บริการการพิสูจน์ตัวตน การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และการยืนยันตัวตน ทั้งนี้ ผู้พิสูจน์และยืนยันตัวตน (IdP) อาจออกสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ภายในกิจการของหน่วยงานหรือให้บริการแก่บุคคลภายนอกก็ได้

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

2.11 แหล่งข้อมูลที่น่าเชื่อถือ (authoritative source: AS) หมายถึง หน่วยงานที่มีการให้หรือจัดทำข้อมูลเกี่ยวกับอัตลักษณ์ที่ถูกต้อง เพื่อให้ IdP สามารถใช้ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลหรือตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์ได้

2.12 ผู้ใช้บริการ (subscriber) หมายถึง บุคคลที่ผ่านการพิสูจน์ตัวตนและได้รับสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ในการยืนยันตัวตน

2.13 ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL) หมายถึง ระดับความมั่นใจหรือระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของบุคคล

2.14 ระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL) หมายถึง ระดับความมั่นใจหรือระดับความเข้มงวดในกระบวนการยืนยันตัวตนของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตน

3. การพิสูจน์และยืนยันตัวตนทางดิจิทัล

3.1 ภาพรวม

ดิจิทัลไอดี (digital identity) คือ อัตลักษณ์ (identity) ของบุคคล ซึ่งใช้บ่งบอกหรือจำแนกบุคคลในการทำธุรกรรมออนไลน์ ทั้งนี้ ดิจิทัลไอดีแต่ละอันจะต้องมีความเฉพาะเจาะจงภายในบริบทของบริการธุรกรรมหนึ่ง ๆ แต่ไม่จำเป็นต้องมีความเฉพาะเจาะจงภายในบริบทของบริการธุรกรรมทั้งหมด กล่าวคือ บริการธุรกรรมบางประเภทอาจไม่จำเป็นต้องทราบข้อมูลเกี่ยวกับอัตลักษณ์ที่แท้จริงของผู้ใช้บริการก็ได้ เช่น การให้บริการอีเมลหรือสื่อสังคมออนไลน์ ขณะที่บริการธุรกรรมประเภทที่มีความเสี่ยงสูง เช่น การให้บริการทางการเงิน ผู้ให้บริการจะต้องทราบข้อมูลเกี่ยวกับอัตลักษณ์ที่แท้จริงของผู้ใช้บริการสำหรับใช้เป็นดิจิทัลไอดีในการทำธุรกรรมออนไลน์

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

บุคคลที่ผ่านการพิสูจน์ตัวตนเรียบร้อยแล้วจะเปลี่ยนสถานะเป็น “ผู้ใช้บริการ (subscriber)” และได้รับสิ่งที่ใช้ยืนยันตัวตน (authenticator) เพื่อใช้ในการยืนยันอัตลักษณ์ของบุคคล เมื่อผู้ใช้บริการต้องการเข้าใช้บริการหรือทำธุรกรรมออนไลน์กับผู้อาศัยการยืนยันตัวตน (relying party: RP) ซึ่งเป็นผู้ให้บริการที่ต้องการทราบอัตลักษณ์ของผู้ใช้บริการก่อนตัดสินใจที่จะให้บริการธุรกรรมดังกล่าว RP จะขอให้ IdP ที่ผู้ใช้บริการเคยผ่านการพิสูจน์ตัวตนและได้รับสิ่งที่ใช้ยืนยันตัวตนมาก่อน ช่วยดำเนินการยืนยันตัวตนของผู้ใช้บริการ

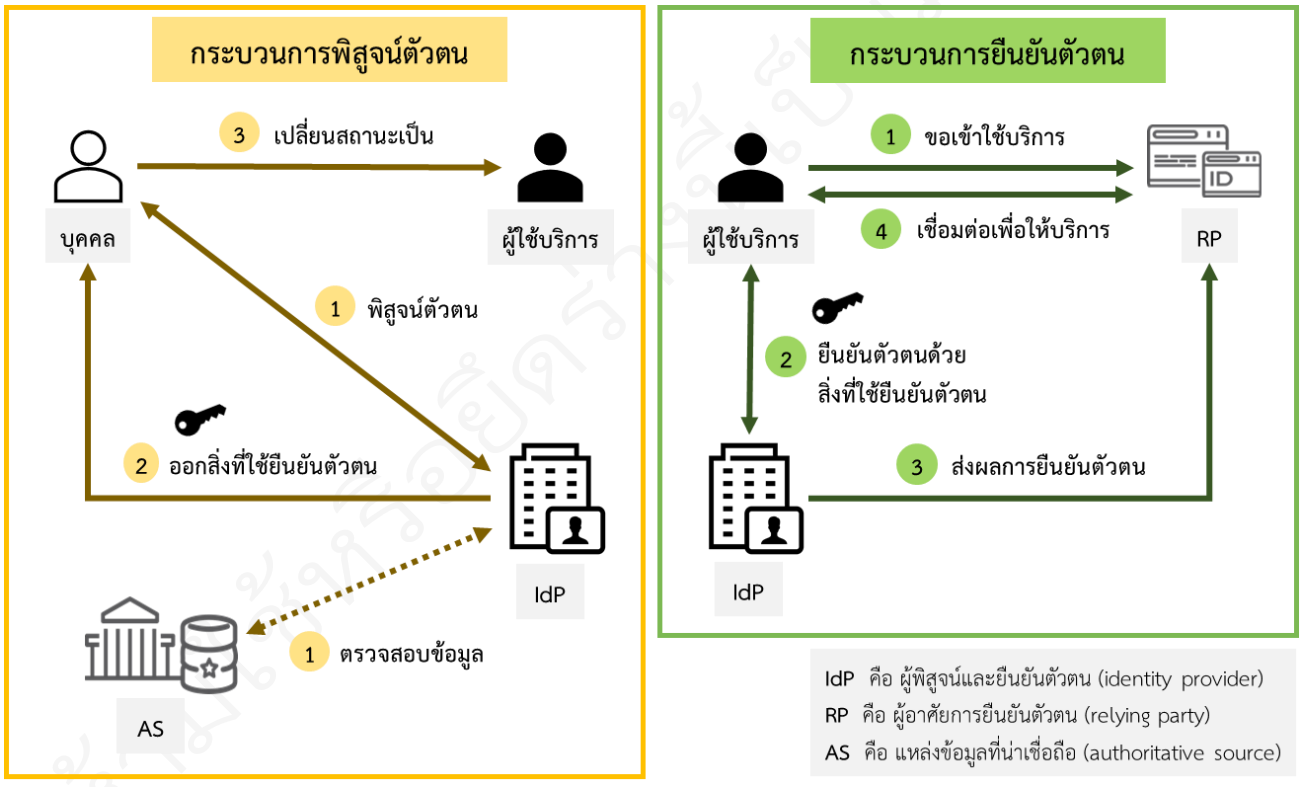
การยืนยันตัวตน (authentication) เป็นกระบวนการที่ IdP ตรวจสอบสิ่งที่ใช้ยืนยันตัวตน โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าบุคคลที่กำลังเข้าใช้บริการเป็นเจ้าของหรือครอบครองสิ่งที่ใช้ยืนยันตัวตนนั้นจริง

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

เมื่อผู้ใช้บริการสามารถยืนยันตัวตนกับ IdP ได้ว่าตนเองเป็นเจ้าของหรือครอบครองสิ่งที่ใช้ยืนยันตัวตนจริงตามเกณฑ์วิธี (protocol) ที่กำหนด IdP จะส่งผลการยืนยันตัวตน (assertion) ให้กับ RP เพื่อใช้ในการตัดสินใจที่จะให้บริการธุรกรรมหรือให้สิทธิในการเข้าใช้งานระบบ โดยผลการยืนยันตัวตนอาจประกอบด้วยข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการ 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) บุคคลที่ประสงค์จะมีดิจิทัลไอดีสำหรับการทำธุรกรรมออนไลน์มาแสดงตนกับ IdP ซึ่ง IdP จะพิสูจน์ตัวตนของบุคคลตามระดับ IAL ที่กำหนด โดยอาจมีการตรวจสอบหลักฐานแสดงตนและข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลกับ AS รวมถึงการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์นั้น

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

(3) บุคคลที่ผ่านการพิสูจน์ตัวตนแล้วจะเปลี่ยนสถานะเป็นผู้ใช้บริการ และมีหน้าที่ดูแลรักษาสิ่งที่ใช้ยืนยันตัวตนของตนเอง

กระบวนการยืนยันตัวตนซึ่งเกิดขึ้นเมื่อผู้ใช้บริการต้องการเข้าใช้บริการหรือทำธุรกรรมออนไลน์กับ RP มีขั้นตอนทั่วไป ดังนี้

(1) ผู้ใช้บริการขอเข้าใช้บริการหรือทำธุรกรรมออนไลน์กับ RP โดยใช้ดิจิทัลไอดีที่มีระดับ IAL และ AAL สอดคล้องตามความต้องการของ RP

(2) RP นำทาง (redirect) ผู้ใช้บริการไปยังหน้าต่างยืนยันตัวตนของ IdP ที่ผู้ใช้บริการเคยผ่านการพิสูจน์ตัวตนมาก่อน และให้ผู้ใช้บริการยืนยันตัวตนกับ IdP ว่าตนเองเป็นเจ้าของหรือครอบครองสิ่งที่ใช้ยืนยันตัวตนตามเกณฑ์วิธีหรือระดับ AAL ที่กำหนด

(3) IdP ตรวจสอบความถูกต้องและสถานะของสิ่งที่ใช้ยืนยันตัวตน แล้วส่งผลการยืนยันตัวตนให้กับ RP ซึ่ง RP สามารถใช้ข้อมูลจากผลการยืนยันตัวตนในการตัดสินใจที่จะให้บริการธุรกรรมหรือให้สิทธิในการเข้าใช้งานระบบกับผู้ใช้บริการ

(4) RP ทำการเชื่อมต่อกับผู้ใช้บริการเพื่อให้บริการธุรกรรมออนไลน์หรือให้เข้าใช้งานระบบ

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

3.3 สิ่งที่ใช้ยืนยันตัวตน

สิ่งที่ใช้ยืนยันตัวตน (authenticator) คือ สิ่งที่ผู้ใช้บริการเป็นเจ้าของหรือครอบครองเพื่อใช้ในการยืนยันตัวตนกับ IdP 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) ก็ได้ โดยความเข้มงวดของการยืนยันตัวตน

จะขึ้นอยู่กับจำนวนปัจจัยของการยืนยันตัวตนและความสามารถในการป้องกันการโจมตีของสิ่งที่ใช้ยืนยันตัวตน อย่างไรก็ตาม IdP และ RP อาจใช้ข้อมูลประเภทอื่น ๆ เช่น ข้อมูลระบุตำแหน่ง หรือข้อมูลระบุอุปกรณ์ที่บุคคลใช้งาน ประกอบเพื่อเพิ่มความมั่นคงปลอดภัยของการยืนยันตัวตน แต่ข้อมูลเหล่านี้ไม่ถือเป็นปัจจัยของการยืนยันตัวตน

ในการยืนยันตัวตนผ่านทางออนไลน์ ผู้ใช้บริการต้องแสดงให้เห็นว่าตนเองเป็นเจ้าของหรือครอบครองสิ่งที่ใช้ยืนยันที่ได้ลงทะเบียนไว้กับ IdP เพื่อยืนยันว่าตนเองเป็นเจ้าของอัตลักษณ์ที่กล่าวอ้างจริง เนื่องจากสิ่งที่ใช้ยืนยันตัวตนจะบรรจุข้อมูลลับ (secret) ที่เฉพาะผู้ใช้บริการตัวจริงเท่านั้นสามารถนำมาใช้ยืนยันตัวตนได้ ทั้งนี้ ข้อมูลลับที่บรรจุอยู่ในสิ่งที่ใช้ยืนยันตัวตนสามารถเป็นกุญแจอสมมาตร (asymmetric keys) หรือข้อมูลลับใช้ร่วมกัน (shared secret) ก็ได้

กรณีที่ข้อมูลลับเป็นกุญแจอสมมาตรซึ่งประกอบด้วยกุญแจส่วนตัว (private key) และกุญแจสาธารณะ (public key) ที่สัมพันธ์กัน ผู้ใช้บริการจะใช้กุญแจส่วนตัวที่บรรจุอยู่ในสิ่งที่ใช้ยืนยันตัวตนเพื่อยืนยันตัวตน ส่วน IdP จะใช้กุญแจสาธารณะที่สัมพันธ์กับกุญแจส่วนตัวเพื่อยืนยันว่าผู้ใช้บริการเป็นเจ้าของหรือครอบครองสิ่งที่ใช้ยืนยันตัวตนที่บรรจุกุญแจส่วนตัวนั้น (โดยทั่วไป กุญแจสาธารณะจะบรรจุอยู่ในใบรับรองกุญแจสาธารณะ (public key certificate))

ในกรณีที่ข้อมูลลับเป็นข้อมูลลับใช้ร่วมกัน ข้อมูลลับที่บรรจุอยู่ในสิ่งที่ใช้ยืนยันตัวตนอาจเป็นกุญแจสมมาตร (symmetric keys) หรือรหัสลับจดจำ (memorized secret) โดยข้อแตกต่างระหว่างกุญแจสมมาตรและรหัสลับจดจำ คือ กุญแจสมมาตรถูกเลือกจากระบบสุ่มและเก็บไว้ในฮาร์ดแวร์หรือซอฟต์แวร์ที่ผู้ใช้บริการครอบครอง ขณะที่รหัสลับจดจำเป็นข้อมูลลับที่ให้ผู้ใช้บริการจดจำ ซึ่งโดยทั่วไป กุญแจเข้ารหัส (cryptographic key) ไม่ว่าจะเป็นกุญแจสมมาตรหรือกุญแจอสมมาตรมักจะมีความยาวของอักขระมากกว่ารหัสลับจดจำ จึงทำให้มีความซับซ้อนที่ยากแก่การคาดเดาโดยผู้ไม่ประสงค์ดี

หมายเหตุ: ปัจจัยของการยืนยันตัวตนบางอย่างไม่สามารถนำมาใช้กับการยืนยันตัวตนผ่านทางออนไลน์ได้โดยตรง เช่น หลักฐานแสดงตนที่ไม่บรรจุข้อมูลลับ แม้จะถือเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณมี และอาจใช้ยืนยันตัวตนแบบพบเห็นต่อหน้ากับบุคคล (เช่น ใช้ยืนยันตัวตนกับเจ้าหน้าที่รักษาความปลอดภัย) แต่ไม่ถือเป็นสิ่งที่ใช้ยืนยันตัวตนสำหรับการยืนยันตัวตนผ่านทางออนไลน์ตามมาตรฐานฉบับนี้

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

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

(2) การใช้ปัจจัยของการยืนยันตัวตนบางปัจจัยเพื่อปกป้องข้อมูลลับที่จะใช้แสดงต่อ IdP เช่น การใช้ลายนิ้วมือ (สิ่งที่คุณเป็น) เพื่อปกป้องกุญแจส่วนตัวที่บรรจุอยู่ในโทรศัพท์เคลื่อนที่ (สิ่งที่คุณมี) โดยผู้ใช้บริการต้องสแกนลายนิ้วมือเพื่อทำให้โทรศัพท์เคลื่อนที่สามารถเรียกใช้กุญแจส่วนตัวในการสร้างข้อมูลยืนยันตัวตนสำหรับแสดงต่อ IdP

3.4 ผลการยืนยันตัวตน

หากการยืนยันตัวตนสำเร็จ IdP จะส่งผลการยืนยันตัวตน (assertion) ให้กับ RP โดยผลการยืนยันตัวตนประกอบด้วยผลการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน และอาจรวมถึงข้อมูลเกี่ยวกับอัตลักษณ์ของผู้ใช้บริการ 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) ของข้อมูลส่วนบุคคลของผู้ใช้บริการที่บรรจุอยู่ในผลการยืนยันตัวตน เพื่อให้มั่นใจว่าเฉพาะ RP ที่กำหนดเท่านั้นสามารถเข้าถึงข้อมูลได้

3.5 ดิจิทัลไอดีแบบ Federated Identity

ดิจิทัลไอดีแบบ federated identity เป็นรูปแบบการใช้งานดิจิทัลไอดีที่ผู้ใช้บริการสามารถให้ IdP ส่งผลการยืนยันตัวตนเกี่ยวกับผู้ใช้บริการให้กับ RP ที่เป็นคนละระบบหรือคนละหน่วยงานได้ รวมถึง RP อาจพึ่งพาอาศัยผลการยืนยันตัวตนจาก IdP มากกว่าหนึ่งรายก็ได้ การใช้งานดิจิทัลไอดีแบบ federated identity มีประโยชน์หลายอย่าง เช่น

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

(2) ลดค่าใช้จ่ายให้กับหน่วยงานในการพัฒนาโครงสร้างพื้นฐานทางเทคโนโลยี (เช่น การบริหารจัดการบัญชีผู้ใช้งานและสิ่งที่ใช้ยืนยันตัวตน) และลดค่าใช้จ่ายให้กับผู้ใช้บริการในการดูแลรักษาสิ่งที่ใช้ยืนยันตัวตน เนื่องจากหน่วยงานในกลุ่มเดียวกันสามารถอาศัยสิ่งที่ใช้ยืนยันตัวตนหรือข้อมูลเกี่ยวกับอัตลักษณ์บางรายการของผู้ใช้บริการร่วมกันได้

(3) ทำให้หน่วยงานสามารถมุ่งเน้นการดำเนินงานไปที่ภารกิจหลักของหน่วยงานโดยตรง แทนที่การดำเนินงานด้านการพิสูจน์และยืนยันตัวตน

4. การกำหนดระดับความน่าเชื่อถือ

4.1 ภาพรวม

ความเสี่ยงที่เกี่ยวข้องการพิสูจน์และยืนยันตัวตนตามมาตรฐานฉบับนี้ แบ่งออกเป็น 2 ด้าน คือ ความเสี่ยงของการพิสูจน์ตัวตนที่ผิดพลาด (เช่น บุคคลที่มาพิสูจน์ตัวตนแอบอ้างอัตลักษณ์ของบุคคลอื่นหรือใช้หลักฐานแสดงตนปลอม) และความเสี่ยงของการยืนยันตัวตนที่ผิดพลาด (เช่น บุคคลที่แสดงสิ่งที่ใช้ยืนยันตัวตน

ไม่ใช่เจ้าของสิ่งที่ใช้ยืนยันตัวตนจริง) โดยผลกระทบที่อาจเกิดขึ้นจากความผิดพลาดของการพิสูจน์และยืนยันตัวตนจะส่งผลกระทบ คือ การให้บริการธุกรรมหรือให้สิทธิในการเข้าใช้งานระบบแก่บุคคลที่ไม่ถูกต้อง

ด้วยเหตุนี้ หน่วยงานจึงต้องประเมินความเสี่ยงของการพิสูจน์ตัวตนที่ผิดพลาดและการยืนยันตัวตนที่ผิดพลาด เพื่อให้สามารถกำหนดระดับความน่าเชื่อถือที่เหมาะสมกับแต่ละบริการธุรกรรม และกำหนดกระบวนการและเทคโนโลยีที่จะใช้ให้เป็นไปตามระดับความน่าเชื่อถือแต่ละระดับ

4.2 ระดับความน่าเชื่อถือ

RP ควรกำหนดระดับความน่าเชื่อถือ (assurance level) ของการพิสูจน์ตัวตนและการยืนยันตัวตนสำหรับแต่ละบริการธุรกรรมตามความเสี่ยงของบริการธุรกรรมนั้น มาตรฐานฉบับนี้แบ่งระดับความน่าเชื่อถือเป็น 2 ด้าน ดังนี้

(1) ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน คือ ระดับความมั่นใจหรือระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของบุคคล 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 ระดับความมั่นใจหรือระดับความเข้มงวดในกระบวนการยืนยันตัวตนของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตน การกำหนดระดับ AAL ที่เหมาะสมจะช่วยลดโอกาสของการยืนยันตัวตนที่ผิดพลาด โดยระดับ AAL แบ่งออกเป็น 3 ระดับ คือ AAL1 (ความน่าเชื่อถือต่ำที่สุด) AAL2 และ AAL3 (ความน่าเชื่อถือสูงที่สุด)

รายละเอียดเป็นไปตามมาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 3 ข้อกำหนดของการยืนยันตัวตน

4.3 การประเมินความเสี่ยงเพื่อกำหนดระดับความน่าเชื่อถือ

RP สามารถดำเนินการประเมินความเสี่ยงเพื่อกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL) ให้เหมาะสมกับแต่ละบริการธุรกรรม ซึ่งประกอบด้วย 2 ขั้นตอน คือ (1) การประเมินระดับผลกระทบที่เป็นไปได้ และ (2) การเชื่อมโยงระดับผลกระทบที่เป็นไปได้เข้ากับระดับความน่าเชื่อถือ โดยมีรายละเอียดดังนี้

(1) ขั้นตอนที่ 1: การประเมินระดับผลกระทบที่เป็นไปได้

การประเมินระดับผลกระทบที่เป็นไปได้ (potential impacts) เป็นการพิจารณาผลกระทบที่เป็นไปได้จากการพิสูจน์ตัวตนที่ผิดพลาด (สำหรับการกำหนดระดับ IAL) และผลกระทบที่เป็นไปได้

จากการยืนยันตัวตนที่ผิดพลาด (สำหรับการกำหนดระดับ AAL) โดยประเภทของผลกระทบ (impact categories) แบ่งออกเป็น 6 ด้าน ดังนี้

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

อย่างไรก็ตาม RP อาจพิจารณาประเภทของผลกระทบด้านอื่น ๆ ให้สอดคล้องกับนโยบายด้านความเสี่ยงของหน่วยงาน

การประเมินระดับผลกระทบที่เป็นไปได้จะใช้วิธีการพิจารณาระดับผลกระทบแต่ละด้านที่สามารถเป็นไปได้เมื่อเกิดข้อผิดพลาด ตามตารางที่ 1

ตารางที่ 1 เกณฑ์การประเมินระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด

ด้านของผลกระทบ	ระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด		
	ต่ำ	ปานกลาง	สูง
ความไม่สะดวกสบายและเสื่อมเสียชื่อเสียง	มีความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียงในระยะสั้นและจำกัด	มีความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียงรุนแรงระยะสั้น หรือมีผลปานกลางในระยะยาว	มีความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียงระยะยาวหรือมีผลกระทบหลายบุคคล
ความเสียหายทางการเงิน	มีความเสียหายทางการเงินที่ไม่มีนัยสำคัญ	มีความเสียหายทางการเงินรุนแรง	มีความเสียหายทางการเงินรุนแรงมาก
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบที่จำกัดต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงมากต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	มีการปล่อยข้อมูลส่วนบุคคลหรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับต่ำ	มีการปล่อยข้อมูลส่วนบุคคลหรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับปานกลาง	มีการปล่อยข้อมูลส่วนบุคคลหรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับสูง
ความปลอดภัยของบุคคล	บาดเจ็บเล็กน้อย ไม่ต้องรับการรักษาพยาบาล	มีความเสี่ยงพอสมควรที่จะบาดเจ็บเล็กน้อย หรือมีความเสี่ยงจำกัดที่จะบาดเจ็บซึ่งต้องรับการรักษาพยาบาล	มีความเสี่ยงที่จะบาดเจ็บสาหัส หรือถึงแก่ชีวิต

ด้านของผลกระทบ	ระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด		
	ต่ำ	ปานกลาง	สูง
การละเมิดทางแพ่งหรือทางอาญา	การฝ่าฝืนกฎหมายนั้นเป็นเรื่องเล็กน้อย ซึ่งไม่จำเป็นต้องมีการบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงที่จะถูกบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงสูงที่จะถูกบังคับใช้กฎหมาย

(2) ขั้นตอนที่ 2: การเชื่อมโยงระดับผลกระทบที่เป็นไปได้เข้ากับระดับความน่าเชื่อถือ

ผลการประเมินระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาดในการพิสูจน์ตัวตนและการยืนยันตัวตนจากขั้นตอนที่ 1 จะนำมาเชื่อมโยงเข้ากับระดับความน่าเชื่อถือ IAL และ AAL ตามลำดับ โดยระดับความน่าเชื่อถือ IAL และ AAL ที่เหมาะสมคือระดับที่ครอบคลุมผลกระทบที่เป็นไปได้ทุกด้าน ตามตารางที่ 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 พบว่าระดับความน่าเชื่อถือที่ครอบคลุมผลกระทบที่เป็นไปได้ทุกด้าน 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
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 2 ดังนั้น ระดับความน่าเชื่อถือ AAL ที่เหมาะสมในตัวอย่างนี้ คือ ระดับ AAL2

ภาคผนวก ก. อักษรย่อ

อักษรย่อ	คำเต็ม	คำภาษาไทย
AAL	Authentication Assurance Level	ระดับความน่าเชื่อถือของการยืนยันตัวตน
AS	Authoritative Source	แหล่งข้อมูลที่น่าเชื่อถือ
FMR	False Match Rate	อัตราการตรงกันที่ผิดพลาด
FNMR	False Non-Match Rate	อัตราการไม่ตรงกันที่ผิดพลาด
IAL	Identity Assurance Level	ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน
IdP	Identity Provider	ผู้พิสูจน์และยืนยันตัวตน
OTP	One-Time Password	รหัสผ่านใช้ครั้งเดียว
PIN	Personal Identification Number	เลขรหัสส่วนตัว
RP	Relying Party	ผู้อาศัยการยืนยันตัวตน

บรรณานุกรม

[1] พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม.

[2] ร่างพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. .... (อยู่ระหว่างการพิจารณาของสำนักงานคณะกรรมการกฤษฎีกา)

[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, September 2020, version 1.1.