ETDA สพธอ www.etda.or.th

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ETDA Recommendation on ICT Standard for Electronic Transactions

ขมธอ. 18-2561

ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย - ภาพรวมและอภิธานศัพท์

DIGITAL IDENTITY GUIDELINE FOR THAILAND – OVERVIEW AND GLOSSARY

เวอร์ชัน 1.0

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ICS 35.030

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย - ภาพรวมและอภิธานศัพท์

ขมธอ. 18-2561

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
หมายเลขโทรศัพท์: 0 2123 1234 หมายเลขโทรสาร: 0 2123 1200

ประกาศโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันที่ 28 กันยายน พ.ศ. 2561

คณะทำงานนำร่องการใช้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ประธานคณะทำงานร่วม

นางสาวสิริธิดา พนมวัน ณ อยุธยา	ธนาคารแห่งประเทศไทย
นายชัยชนะ มิตรพันธ์	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

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 (องค์การมหาชน)
นายธนฉัตร วิจารณ์ปรีชา	ธนาคารเกียรตินาคิน จำกัด (มหาชน)

ผู้ช่วยเลขานุการ

นายนครินทร์ ลิ้มรังษี	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ ฉบับนี้ จัดทำขึ้นเพื่ออธิบายภาพรวมของการใช้งานดิจิทัลไอดีภายใต้บริบทของประเทศไทย ตลอดจนกรอบแนวปฏิบัติในการพิสูจน์ตัวตนของบุคคลธรรมดา และการใช้งานสิ่งที่ใช้ยืนยันตัวตน โดยพัฒนาตามแนวมาตรฐานของ NIST Special Publication 800-63-3 – Digital Identity Guidelines, National Institute of Standards and Technology, US Department of Commerce, June 2017 [1]

และได้มีการรับฟังความคิดเห็นจากหน่วยงานที่เกี่ยวข้อง เพื่อปรับปรุงให้ข้อเสนอแนะมาตรฐานฉบับนี้มีความครบถ้วนสมบูรณ์ และสามารถนำไปปรับใช้ในทางปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้งานดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวม และอภิธานศัพท์ ฉบับนี้ จัดทำขึ้นตามความร่วมมือด้านการมาตรฐานระหว่าง หน่วยงานภาครัฐและเอกชนในคณะทำงานนำร่องการใช้ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ร่วมกับ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200
E-mail: estandard.center@etda.or.th
Website: www.etda.or.th

คำนำ

การให้บริการของรัฐแก่ประชาชนและภาคธุรกิจ หรือการให้บริการของภาคธุรกิจแก่ประชาชนในปัจจุบัน ประกอบด้วยขั้นตอนการพิสูจน์และยืนยันตัวตนที่มีความซับซ้อน มีความสิ้นเปลืองทั้งเวลาและทรัพยากร เกิดภาระแก่ทั้งผู้แสดงตนและผู้มีหน้าที่ในการตรวจสอบความถูกต้องและยืนยันตัวตน รัฐบาลจึงได้ดำเนินงานพัฒนาระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID Platform) ที่สอดคล้องกับนโยบายอำนวยความสะดวกในการประกอบธุรกิจ (Ease of Doing Business) และการให้บริการกับประชาชน เพื่อให้เป็นโครงสร้างพื้นฐานทางดิจิทัลที่สำคัญของประเทศ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน ได้ร่วมกันกำหนดแนวทางการพัฒนาระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลของประเทศ และจัดทำมาตรฐานเกี่ยวกับแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย (Digital Identity Guideline for Thailand) ขึ้น ประกอบด้วยมาตรฐานทั้งหมด 3 ฉบับ ดังนี้

(1) แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ (Overview and Glossary)

เป็นเอกสารอธิบายภาพรวมและอภิธานศัพท์เกี่ยวกับการใช้งานดิจิทัลไอดีสำหรับประเทศไทย การบริหารความเสี่ยง และการกำหนดระดับความน่าเชื่อถือ

(2) แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน (Enrolment and Identity Proofing)

เป็นเอกสารอธิบายข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการลงทะเบียนและพิสูจน์ตัวตนของผู้สมัครใช้บริการที่ประสงค์จะทำธุรกรรมออนไลน์ด้วยดิจิทัลไอดี (digital identity) ตามระดับความน่าเชื่อถือของไอเดนทิตี (identity assurance level: IAL)

(3) แนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน (Authentication)

เป็นเอกสารอธิบายข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ในการกำหนดและบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน (authenticator) ตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (authenticator assurance level: AAL)

สารบัญ

สารบัญรูป

สารบัญตาราง

ETDA
สพธอ
www.etda.or.th

ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
เรื่อง ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์

ตามที่สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้ประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ ลงวันที่ ๒๘ กันยายน พ.ศ. ๒๕๖๑ นั้น เนื่องจากมีถ้อยคำที่สมควรแก้ไข จึงให้ยกเลิกประกาศดังกล่าว ทั้งนี้ เพื่อให้มีแนวทางการอธิบายภาพรวมและอภิธานศัพท์ ที่เกี่ยวกับการใช้งานดิจิทัลไอดีภายใต้บริบทของประเทศไทย ตลอดจนเป็นกรอบแนวปฏิบัติในการพิสูจน์ตัวตนของบุคคลธรรมดา และการใช้งานสิ่งที่ใช้ยืนยันตัวตน

อาศัยอำนาจตามความในมาตรา ๗ (๔) แห่งพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พ.ศ. ๒๕๕๔ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) จึงประกาศข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – ภาพรวมและอภิธานศัพท์ เลขที่ ขมธอ. ๑๘-๒๕๖๑ ปรากฏตามท้ายประกาศฉบับนี้ ทั้งนี้ ตั้งแต่วันที่ ๒๘ กันยายน พ.ศ. ๒๕๖๑ เป็นต้นไป

ประกาศ ณ วันที่ ๑๑ กุมภาพันธ์ พ.ศ. ๒๕๖๒

(นางสุรางคณา วายุภาพ)
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์

ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย - ภาพรวมและอภิธานศัพท์

1. ขอบข่าย

ข้อเสนอแนะมาตรฐานฉบับนี้ จัดทำขึ้นเพื่ออธิบายภาพรวมและอภิธานศัพท์เกี่ยวกับการใช้ดิจิทัลไอดีสำหรับประเทศไทยเพื่อให้หน่วยงานที่เกี่ยวข้องกับการใช้งานดิจิทัลไอดีมีความเข้าใจตรงกัน โดยเนื้อหาของเอกสารนี้จะครอบคลุมถึงแบบจำลองของดิจิทัลไอดี (digital identity model) และการบริหารความเสี่ยงของดิจิทัลไอดี

2. บทนิยาม

ความหมายของคำที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

2.1 คุณลักษณะ (attribute) หมายถึง ลักษณะ (characteristic) หรือคุณสมบัติ (property) ของบุคคล [1]

2.2 ไอเดนทิตี (identity หรือ ID) หมายถึง คุณลักษณะ หรือชุดของคุณลักษณะที่ใช้ระบุตัวบุคคลในบริบทที่กำหนด [1]

2.3 ดิจิทัลไอดี (digital identity หรือ digital ID) หมายถึง คุณลักษณะ หรือชุดของคุณลักษณะที่ถูกรวบรวมและบันทึกในรูปแบบดิจิทัล ซึ่งสามารถใช้ระบุตัวบุคคลในบริบทที่กำหนด และสามารถใช้ทำธุรกรรมอิเล็กทรอนิกส์ [2]

2.4 สิ่งที่ใช้ยืนยันตัวตน (authenticator) หมายถึง สิ่งที่ผู้ใช้บริการครอบครองเพื่อใช้ในการยืนยันตัวตน โดยสิ่งที่ใช้ยืนยันตัวตนจะมีปัจจัยของการยืนยันตัวตนอย่างน้อยหนึ่งปัจจัย

2.5 สิ่งที่ใช้รับรองตัวตน (credential) หมายถึง เอกสาร วัตถุ (object) หรือกลุ่มข้อมูล (data structure) ที่เชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตน ตัวอย่างเช่น หนังสือเดินทาง บัตรประจำตัวประชาชน หรือ ใบรับรองอิเล็กทรอนิกส์ (digital certificate) [1]

2.6 ผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) หมายถึง บุคคลหรือหน่วยงานที่น่าเชื่อถือซึ่งทำหน้าที่

(1) รับลงทะเบียน (enrolment) และพิสูจน์ตัวตน (identity proofing) และ
(2) บริหารจัดการสิ่งที่ใช้รับรองตัวตน (credential) ซึ่งเชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตน (authenticator) ของผู้ใช้บริการ

โดยผู้พิสูจน์และยืนยันตัวตนอาจบริหารจัดการสิ่งที่ใช้รับรองตัวตนเพื่อใช้ภายในองค์กรหรือใช้ภายนอกองค์กรก็ได้

2.7 ผู้ให้บริการ (relying party: RP) หมายถึง บุคคลหรือหน่วยงานซึ่งให้บริการทำธุรกรรม หรืออนุญาตให้เข้าถึงข้อมูลหรือระบบ โดยอาศัย (1) สิ่งที่ใช้ยืนยันตัวตน (authenticator) และ (2) ผลการยืนยันตัวตน (assertion) หรือสิ่งที่ใช้รับรองตัวตน (credential) จากผู้พิสูจน์และยืนยันตัวตน

2.8 ผู้ให้ข้อมูลที่น่าเชื่อถือ (authoritative source: AS) หมายถึง บุคคลหรือหน่วยงานที่มีความน่าเชื่อถือและสามารถเข้าถึงหรือมีข้อมูลที่ถูกต้อง และทำหน้าที่

(1) ตรวจสอบข้อมูลหรือสถานะของหลักฐานแสดงตนของผู้ใช้บริการตามการร้องขอจากผู้พิสูจน์และยืนยันตัวตน หรือ

(2) อนุญาตให้ผู้ให้บริการเข้าถึงข้อมูลที่น่าเชื่อถือ หรือข้อมูลส่วนบุคคลซึ่งได้รับความยินยอมจากผู้ใช้บริการ

2.9 ผู้สมัครใช้บริการ (applicant) หมายถึง บุคคลที่สมัครใช้บริการพิสูจน์และยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน

2.10 ผู้ใช้บริการ (subscriber) หมายถึง ผู้สมัครใช้บริการที่ผ่านการลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตน และได้รับสิ่งที่ใช้ยืนยันตัวตนสำหรับใช้ยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน

2.11 การลงทะเบียน (enrolment)[1] หมายถึง กระบวนการที่ผู้สมัครใช้บริการลงทะเบียนเป็นผู้ใช้บริการของผู้พิสูจน์และยืนยันตัวตน

2.12 การพิสูจน์ตัวตน (identity proofing) หมายถึง กระบวนการที่ผู้พิสูจน์และยืนยันตัวตนรวบรวมข้อมูล ตรวจสอบหลักฐานแสดงตน และตรวจสอบตัวตนของผู้สมัครใช้บริการ

2.13 การยืนยันตัวตน (authentication) หมายถึง กระบวนการที่ผู้ใช้บริการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตนว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างด้วยการใช้สิ่งที่ใช้ยืนยันตัวตน (authenticator)

2.14 การอนุญาตเฉพาะผู้มีสิทธิเข้าถึง (authorization) หมายถึง กระบวนการที่ผู้ใช้บริการอนุญาตให้ผู้ให้บริการเข้าถึงข้อมูลของตน

3. อักษรย่อ

อักษรย่อที่ใช้ในข้อเสนอแนะมาตรฐานฉบับนี้ มีดังต่อไปนี้

อักษรย่อ	คำเต็ม	คำภาษาไทย
AAL	authenticator assurance level	ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน
AS	authoritative source	ผู้ให้ข้อมูลที่น่าเชื่อถือ
IAL	identity assurance level	ระดับความน่าเชื่อถือของไอเดนทิตี
IdP	identity provider	ผู้พิสูจน์และยืนยันตัวตน
KBV	knowledge-based verification	การยืนยันด้วยชุดข้อมูลที่รู้เฉพาะผู้สมัครใช้บริการ
OTP	one-time password	รหัสผ่านแบบใช้ครั้งเดียว

[1] กรณีที่อ้างอิงถึงมาตรฐานของ NIST Special Publication 800-63A จะสะกดว่า “enrollment”

อักษรย่อ	คำเต็ม	คำภาษาไทย
PAD	presentation attack detection	การตรวจจับการปลอมแปลงชีวมิติ
PIN	personal identification number	เลขรหัสส่วนตัว
RP	relying party	ผู้ให้บริการ

4. แบบจำลองดิจิทัลไอดี (Digital ID Model)

4.1 ภาพรวม

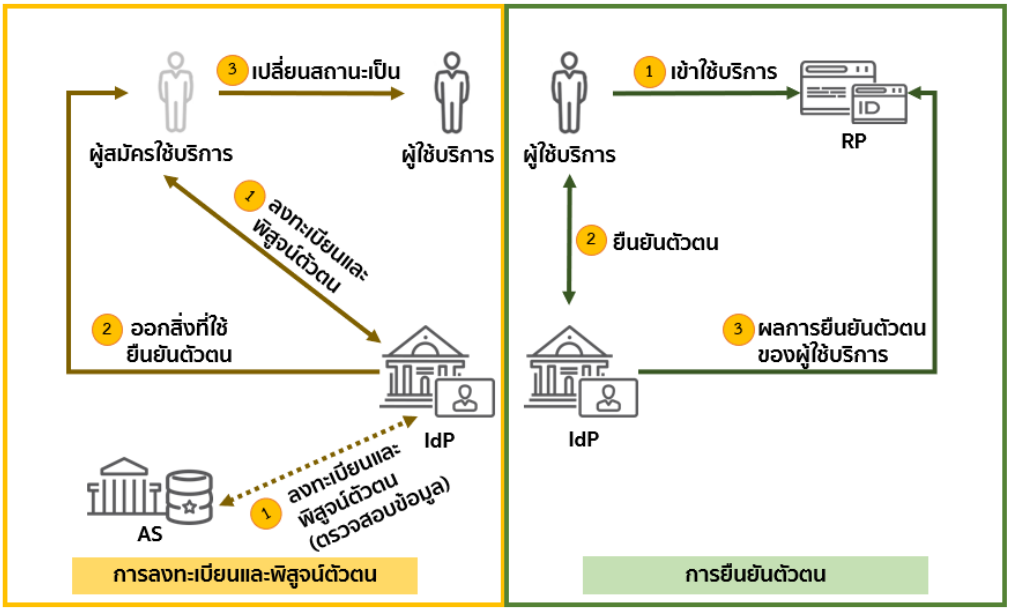
ดิจิทัลไอดี (digital identity) คือ ไอเดนทิตีที่บุคคลใช้แสดงตัวตนเพื่อขอเข้าใช้บริการหรือทำธุรกรรมออนไลน์ ซึ่งดิจิทัลไอดีแต่ละอันจะมีคุณลักษณะเฉพาะที่แตกต่างจากดิจิทัลไอดีอื่น ๆ (unique) ที่อยู่ภายใต้บริการเดียวกัน อย่างไรก็ตาม ดิจิทัลไอดีไม่จำเป็นต้องระบุตัวตนที่แท้จริงของผู้ใช้บริการได้เสมอไป เช่น การใช้ดิจิทัลไอดีสำหรับแสดงตัวตนเพื่อเข้าใช้บริการอีเมลหรือสังคมออนไลน์ (social network) ดิจิทัลไอดีดังกล่าวอาจไม่สามารถระบุตัวบุคคลซึ่งเป็นเจ้าของดิจิทัลไอดีได้ ในขณะที่การใช้ดิจิทัลไอดีสำหรับแสดงตัวตนเพื่อเข้าใช้บริการอิเล็กทรอนิกส์หรือทำธุรกรรมที่มีความเสี่ยงสูง ผู้ให้บริการจะต้องทราบตัวตนที่แท้จริงของผู้ใช้บริการที่เชื่อมโยงกับดิจิทัลไอดี ความเชื่อมโยงระหว่างตัวตนของผู้ใช้บริการกับดิจิทัลไอดีนี้เกิดขึ้นในกระบวนการพิสูจน์ตัวตน (identity proofing)

การใช้งานดิจิทัลไอดีเริ่มต้นจากผู้สมัครใช้บริการ (applicant) ลงทะเบียนใช้บริการพิสูจน์และยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน (identity provider หรือ IdP) ซึ่ง IdP จะลงทะเบียนและพิสูจน์ตัวตนของผู้สมัครใช้บริการตามระดับความเข้มงวดของการพิสูจน์ตัวตน ซึ่งตามข้อเสนอแนะมาตรฐานฉบับนี้เรียกว่า “ระดับความน่าเชื่อถือของไอเดนทิตี (identity assurance level: IAL)” ผู้สมัครใช้บริการที่ผ่านการลงทะเบียนและพิสูจน์ตัวตนเรียบร้อยแล้วจะเปลี่ยนสถานะเป็น “ผู้ใช้บริการ (subscriber)” และได้รับสิ่งที่ใช้ยืนยันตัวตน (authenticator) เพื่อใช้ในกระบวนการยืนยันตัวตน (authentication) กับ IdP

เมื่อผู้ใช้บริการต้องการเข้าใช้บริการหรือทำธุรกรรมออนไลน์กับผู้ให้บริการ (relying party หรือ RP) ที่ต้องการทราบตัวตนของผู้ใช้บริการ ผู้ใช้บริการสามารถขอให้ IdP ที่ตนเองเคยพิสูจน์ตัวตนและได้รับสิ่งที่ใช้ยืนยันตัวตนที่ตรงตามระดับความต้องการของ RP ช่วยยืนยันตัวตนและส่งผลการยืนยันตัวตน (assertion) ให้กับ RP โดยผลการยืนยันตัวตนประกอบด้วยไอเดนทิตีและข้อมูลอื่น ๆ (ที่ผู้ใช้บริการยินยอมให้เปิดเผย) ที่ RP ใช้พิจารณาสิทธิของผู้ใช้บริการ

IdP จะส่งผลการยืนยันตัวตนซึ่งมีข้อมูลเกี่ยวกับผู้ใช้บริการให้กับ RP ก็ต่อเมื่อผู้ใช้บริการสามารถยืนยันตัวตนได้ว่าตนเองคือเจ้าของไอเดนทิตีที่กล่าวอ้างจริง โดยการพิสูจน์ให้ IdP เห็นว่าเป็นผู้ครอบครองสิ่งที่ใช้ยืนยันตัวตนตามเกณฑ์วิธี (protocol) ที่ IdP กำหนด ทั้งนี้ สิ่งที่ใช้ยืนยันตัวตนแต่ละประเภทมีระดับความปลอดภัยจากการโจมตีโดยผู้ไม่ประสงค์ดีแตกต่างกัน ข้อเสนอแนะมาตรฐานฉบับนี้จึงแบ่งสิ่งที่ใช้ยืนยันตัวตนเป็นระดับเรียกว่า “ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (authenticator assurance level: AAL)” ซึ่งเป็นระดับที่บ่งบอกความน่าเชื่อถือว่าผู้ที่ยืนยันตัวตนเป็นบุคคลเดียวกับที่ได้ลงทะเบียนไว้กับ IdP

ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้องในการลงทะเบียนและพิสูจน์ตัวตน และการยืนยันตัวตน แสดงให้เห็นตามรูปที่ 1



รูปที่ 1 แบบจำลองดิจิทัลไอดี

ด้านซ้ายของรูปที่ 1 แสดงกระบวนการลงทะเบียนและพิสูจน์ตัวตน ซึ่งมีขั้นตอนทั่วไป ดังนี้

(1) ผู้สมัครใช้บริการลงทะเบียนเป็นผู้ใช้บริการของ IdP ซึ่ง IdP จะพิสูจน์ตัวตนของผู้สมัครใช้บริการตามระดับความน่าเชื่อถือของไอเดนทิตีที่กำหนด โดยอาจตรวจสอบข้อมูลกับผู้ให้ข้อมูลที่น่าเชื่อถือ (authoritative source: AS)

(2) หากการพิสูจน์ตัวตนสำเร็จ IdP จะสร้างหรือลงทะเบียนสิ่งที่ใช้ยืนยันตัวตน และสร้างสิ่งที่ใช้รับรองตัวตนซึ่งเป็นข้อมูลเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตีของผู้ใช้บริการ

(3) ผู้สมัครใช้บริการเปลี่ยนสถานะเป็น “ผู้ใช้บริการ” โดย IdP จะเก็บรักษาสิ่งที่ใช้รับรองตัวตน สถานะของสิ่งที่ใช้รับรองตัวตน และข้อมูลที่ผู้ใช้บริการใช้ลงทะเบียน ตลอดอายุการใช้งานของสิ่งที่ใช้รับรองตัวตน (เป็นอย่างน้อย) ส่วนผู้ใช้บริการเก็บรักษาสิ่งที่ใช้ยืนยันตัวตน

ด้านขวาของรูปที่ 1 แสดงกระบวนการยืนยันตัวตนที่เกิดขึ้นเมื่อผู้ใช้บริการต้องการเข้าใช้บริการหรือทำธุรกรรมกับ RP ซึ่งมีขั้นตอนทั่วไปดังนี้

(1) ผู้ใช้บริการขอเข้าใช้บริการหรือทำธุรกรรมออนไลน์กับ RP โดยใช้ดิจิทัลไอดีที่มีระดับความน่าเชื่อถือของไอเดนทิตีและระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนตรงตามความต้องการของ RP

(2) ผู้ใช้บริการยืนยันตัวตนว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างจริง โดยพิสูจน์ให้ IdP เห็นว่าตนครอบครองสิ่งที่ใช้ยืนยันตัวตนตามเกณฑ์วิธีที่ IdP กำหนด

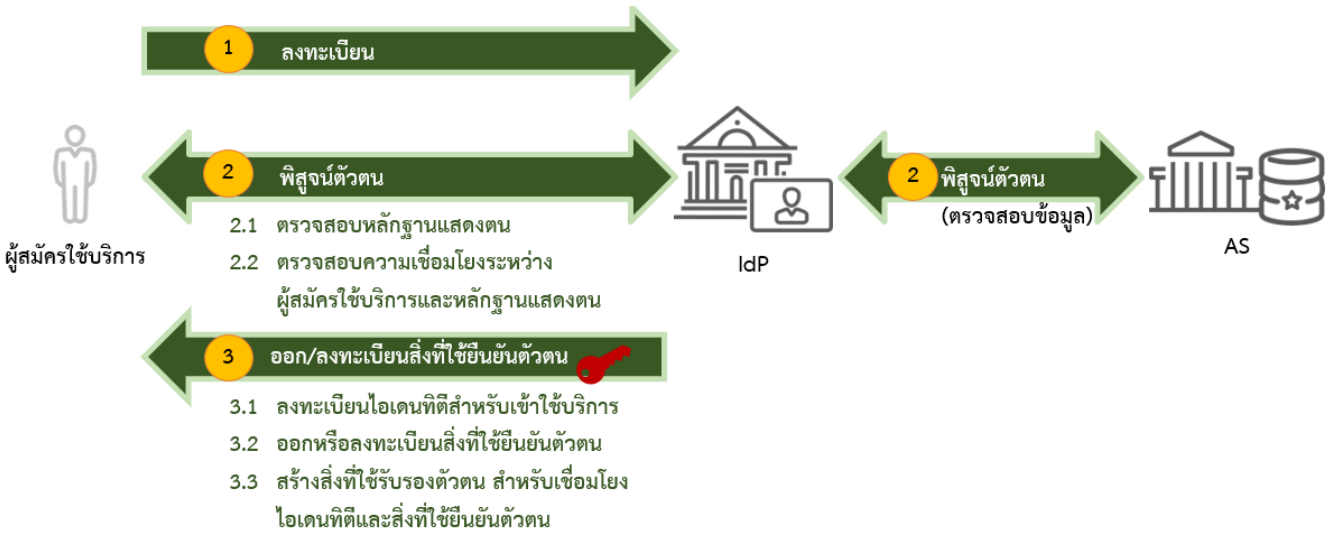
(3) IdP ตรวจสอบความถูกต้องและสถานะของสิ่งที่ใช้ยืนยันตัวตนและสิ่งที่ใช้รับรองตัวตน แล้วส่งผลการยืนยันตัวตนให้กับ RP ซึ่ง RP สามารถใช้ข้อมูลที่อยู่ในผลการยืนยันตัวตนนี้พิจารณาสิทธิต่าง ๆ ของผู้ใช้บริการ

(4) RP ทำการเชื่อมต่อกับผู้ใช้บริการ

4.2 การลงทะเบียนและพิสูจน์ตัวตน

การใช้งานดิจิทัลไอดีเริ่มต้นจากการที่ผู้สมัครใช้บริการลงทะเบียนกับ IdP ที่ตนต้องการใช้บริการพิสูจน์และยืนยันตัวตน จากนั้น IdP จะดำเนินการพิสูจน์ตัวตนผู้สมัครใช้บริการโดยความเข้มงวดขึ้นอยู่กับระดับความน่าเชื่อถือของไอเดนทิตี (รายละเอียดจะกล่าวต่อไปในหัวข้อ 5.2.1) การพิสูจน์ตัวตนของผู้สมัครใช้บริการครอบคลุมถึงการตรวจสอบหลักฐานแสดงตน การตรวจสอบความเชื่อมโยงระหว่างผู้สมัครใช้บริการและหลักฐานแสดงตน และการตรวจสอบข้อมูลของผู้สมัครใช้บริการกับ AS

กระบวนการลงทะเบียนและพิสูจน์ตัวตนเพื่อใช้งานดิจิทัลไอดีมีรายละเอียดตามรูปที่ 2



รูปที่ 2 กระบวนการลงทะเบียนและพิสูจน์ตัวตน

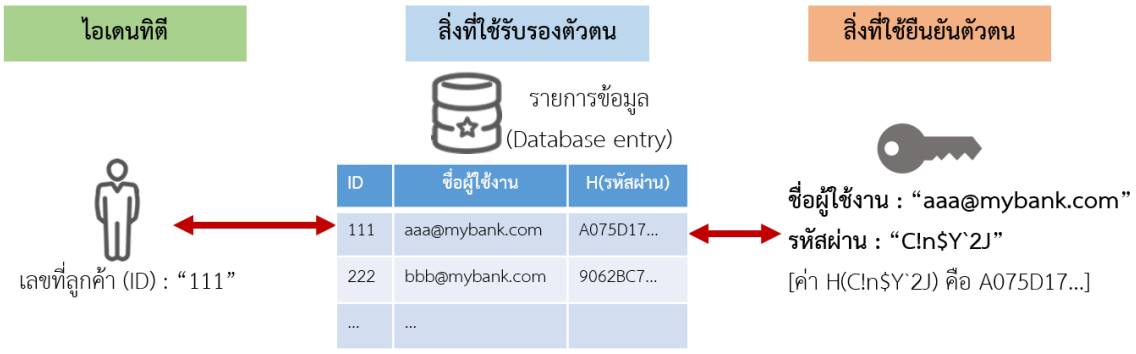
หลังจากการพิสูจน์ตัวตนเรียบร้อยแล้ว IdP จะดำเนินการดังนี้

(1) ลงทะเบียนไอเดนทิตีที่ใช้ระบุตัวตนผู้ใช้บริการแต่ละราย เช่น สร้างเลขประจำตัวให้กับผู้ใช้บริการหรือลงทะเบียนชื่อผู้ใช้บริการ (user ID) ที่ไม่ซ้ำกัน

(2) ออก (issue) หรือลงทะเบียน (register) สิ่งที่ใช้ยืนยันตัวตนให้กับผู้ใช้บริการ โดยชนิดของสิ่งที่ใช้ยืนยันตัวตนขึ้นอยู่กับระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL) ซึ่งรายละเอียดจะกล่าวต่อไปในหัวข้อ 5.2.2

(3) สร้างสิ่งที่ใช้รับรองตัวตน (credential) ซึ่งเป็นข้อมูลที่เชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตีของผู้ใช้บริการ เพื่อให้ผู้ใช้บริการสามารถนำสิ่งที่ใช้ยืนยันตัวตนดังกล่าวมาใช้ยืนยันตัวตนในอนาคต

ตัวอย่างของไอเดนทิตี สิ่งที่ใช้รับรองตัวตนและสิ่งที่ใช้ยืนยันตัวตน มีรายละเอียดตามรูปที่ 3



หมายเหตุ: H(รหัสผ่าน) คือค่าฟังก์ชัน hash ของรหัสผ่าน

รูปที่ 3 ตัวอย่างของไอเดนทิตี สิ่งที่ใช้รับรองตัวตน และสิ่งที่ใช้ยืนยันตัวตน

จากรูปที่ 3 ไอเดนทิตีซึ่งเป็นคุณลักษณะเฉพาะที่แตกต่างระหว่างผู้ใช้บริการแต่ละรายภายใต้ IdP เดียวกัน คือ "เลขที่ลูกค้า (ID)" สิ่งที่ใช้ยืนยันตัวตนที่ผู้ใช้บริการครอบครองเพื่อใช้ยืนยันตัวตน คือ "ชื่อผู้ใช้งานและรหัสผ่าน" และสิ่งที่ใช้รับรองตัวตนที่เชื่อมโยงไอเดนทิตีกับสิ่งที่ใช้ยืนยันตัวตน คือ "รายการข้อมูล (database entry)" ซึ่งบ่งบอกว่าสิ่งที่ใช้ยืนยันตัวตนแต่ละอันเชื่อมโยงไปยังผู้ใช้บริการรายใด

หลังเสร็จสิ้นกระบวนการลงทะเบียนและพิสูจน์ตัวตน ผู้ใช้บริการมีหน้าที่ดูแลรักษาสิ่งที่ใช้ยืนยันตัวตนของตนเองให้ปลอดภัยจากการนำไปใช้งานโดยผู้ที่ไม่ได้รับอนุญาต ในขณะที่ IdP มีหน้าที่เก็บรักษาข้อมูลเกี่ยวกับสิ่งที่ใช้รับรองตัวตนและข้อมูลการลงทะเบียนของผู้ใช้บริการอย่างปลอดภัยและมีสภาพพร้อมใช้งาน

4.3 การยืนยันตัวตน

4.3.1 สิ่งที่ใช้ยืนยันตัวตน

สิ่งที่ใช้ยืนยันตัวตน (authenticator) คือสิ่งที่ผู้ใช้บริการครอบครองและใช้ในการยืนยันตัวตนกับ IdP ว่าเป็นบุคคลที่กล่าวอ้างจริง สิ่งที่ใช้ยืนยันตัวตนอาจประกอบด้วยปัจจัยของการยืนยันตัวตนเพียงหนึ่งปัจจัย (การยืนยันตัวตนแบบปัจจัยเดียว: single-factor authentication) หรือประกอบด้วยปัจจัยของการยืนยันตัวตนมากกว่าหนึ่งปัจจัย (การยืนยันตัวตนแบบหลายปัจจัย: multi-factor authentication) ก็ได้ อย่างไรก็ตาม ความปลอดภัยของระบบยืนยันตัวตน (authentication system) ขึ้นอยู่กับความสามารถในการป้องกันการโจมตีของสิ่งที่ใช้ยืนยันตัวตนและจำนวนปัจจัยของการยืนยันตัวตน โดยปัจจัยของการยืนยันตัวตน (authentication factor) แบ่งออกเป็น 3 ประเภท ดังนี้

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

(2) สิ่งที่ผู้ใช้บริการมี (something you have) คือ สิ่งของที่ผู้ใช้บริการเท่านั้นครอบครอง เช่น กุญแจส่วนตัว (private key) เป็นต้น

(3) สิ่งที่ผู้ใช้บริการเป็น (something you are) คือ ข้อมูลทางชีวมิติ (biometric) ของผู้ใช้บริการ เช่น ลายนิ้วมือ ใบหน้า ม่านตา เสียง เป็นต้น

ในการยืนยันตัวตนผ่านระบบอิเล็กทรอนิกส์ ผู้ใช้บริการต้องพิสูจน์ว่าตนครอบครองสิ่งที่ใช้ยืนยันตัวตนที่ได้ลงทะเบียนไว้กับ IdP เพื่อยืนยันว่าตนเองเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างจริง โดยสิ่งที่ใช้ยืนยันตัวตนจะมีข้อมูลลับที่เฉพาะผู้ใช้บริการตัวจริงเท่านั้นครอบครองหลังจากการลงทะเบียนและพิสูจน์ตัวตนกับ IdP

ข้อมูลลับภายใต้สิ่งที่ใช้ยืนยันตัวตนสามารถเป็นกุญแจสมมาตร (symmetric key) หรือกุญแจอสมมาตร (asymmetric key) ก็ได้ กรณีที่เป็นกุญแจอสมมาตร ผู้ใช้บริการจะใช้กุญแจส่วนตัว (private key) ซึ่งบรรจุในสิ่งที่ใช้ยืนยันตัวตนเพื่อยืนยันตัวตน ส่วน IdP จะใช้กุญแจสาธารณะ (public key) ที่บรรจุในสิ่งที่ใช้รับรองตัวตน (credential) ซึ่งโดยทั่วไปคือ ใบรับรองกุญแจสาธารณะ (public key certificate) เพื่อตรวจสอบความถูกต้องของกุญแจส่วนตัวของผู้ใช้บริการ ในกรณีที่ข้อมูลลับเป็นกุญแจสมมาตร ข้อมูลลับที่บรรจุในสิ่งที่ใช้ยืนยันตัวตนอาจเป็นกุญแจ (key) หรือรหัสลับจดจำ (memorized secret) โดยข้อแตกต่างระหว่างกุญแจและรหัสลับจดจำคือ กุญแจมักสร้างจากระบบสุ่มและเก็บไว้ในอุปกรณ์ฮาร์ดแวร์หรือซอฟต์แวร์ ในขณะที่รหัสลับจดจำเป็นข้อมูลที่ผู้ใช้บริการสามารถจดจำได้

การยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) สามารถทำได้ 2 รูปแบบ คือ

(1) การแสดงปัจจัยของการยืนยันตัวตนแต่ละปัจจัยต่อ IdP โดยตรง เช่น ผู้ใช้บริการต้องแสดงรหัสผ่าน (สิ่งที่ผู้ใช้บริการรู้) และรหัสผ่านแบบใช้ครั้งเดียวที่ได้รับทางโทรศัพท์เคลื่อนที่ (สิ่งที่ผู้ใช้บริการมี) เพื่อยืนยันตัวตน

(2) การใช้ปัจจัยของการยืนยันตัวตนบางปัจจัยเพื่อปกป้องข้อมูลลับที่ใช้ยืนยันตัวตนกับ IdP เช่น การใช้ลายนิ้วมือ (สิ่งที่ผู้ใช้บริการเป็น) เพื่อปกป้องกุญแจส่วนตัวที่บรรจุในอุปกรณ์ฮาร์ดแวร์ (สิ่งที่ผู้ใช้บริการมี) เมื่อต้องการยืนยันตัวตน ผู้ใช้บริการต้องประทับลายนิ้วมือเพื่อทำให้อุปกรณ์ฮาร์ดแวร์สามารถใช้งานกุญแจส่วนตัวสร้างข้อมูลสำหรับยืนยันตัวตน

4.3.2 สิ่งที่ใช้รับรองตัวตน

สิ่งที่ใช้รับรองตัวตน (credential) คือ เอกสาร วัตถุ (object) หรือกลุ่มข้อมูล (data structure) ที่เชื่อมโยงไอเดนทิตีของผู้ใช้บริการเข้ากับสิ่งที่ใช้ยืนยันตัวตน ผู้ใช้บริการต้องครอบครองสิ่งที่ใช้ยืนยันตัวตน แต่ไม่จำเป็นต้องครอบครองสิ่งที่ใช้รับรองตัวตน

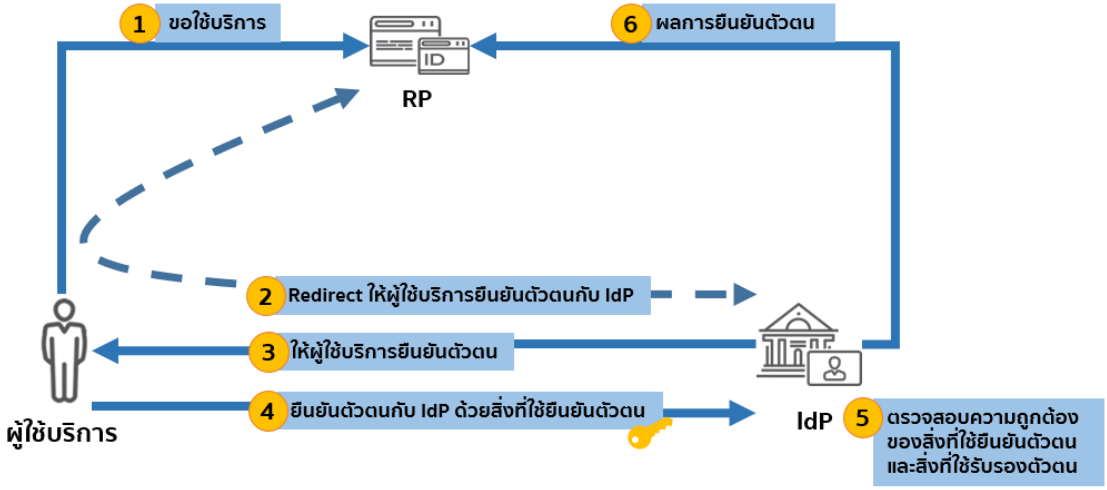
ตัวอย่างของสิ่งที่ใช้รับรองตัวตนที่ผู้ใช้บริการไม่ได้ครอบครอง เช่น ฐานข้อมูลที่เชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนกับไอเดนทิตีของผู้ใช้บริการ (สิ่งที่ใช้ยืนยันตัวตนคือ รหัสผ่าน)

ตัวอย่างของสิ่งที่ใช้รับรองตัวตนที่ผู้ใช้บริการครอบครอง เช่น ใบรับรองกุญแจสาธารณะ (สิ่งที่ใช้ยืนยันตัวตน คือ กุญแจส่วนตัว และ PIN สำหรับใช้งานกุญแจส่วนตัว))

4.3.3 กระบวนการยืนยันตัวตน

เมื่อผู้ใช้บริการต้องการขอเข้าใช้บริการหรือทำธุรกรรมออนไลน์ซึ่งต้องการทราบไอเดนทิตีของผู้ใช้บริการ ผู้ใช้บริการสามารถยืนยันตัวตนกับ IdP โดยแสดงให้เห็นว่าตนครอบครองสิ่งที่ใช้ยืนยันตัวตนซึ่งเชื่อมโยงกับไอเดนทิตีที่กล่าวอ้างตามเกณฑ์วิธีที่ IdP กำหนด และตรงตามระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนที่ RP ต้องการ จากนั้น IdP จะตรวจสอบความถูกต้องของสิ่งที่ใช้ยืนยันตัวตนและสิ่งที่ใช้รับรองตัวตน แล้วส่งผลการยืนยันตัวตนให้กับ RP

รูปที่ 4 แสดงตัวอย่างกระบวนการยืนยันตัวตน ซึ่งเริ่มจากผู้ใช้บริการเข้าใช้บริการบนเว็บไซต์ของ RP ซึ่ง RP ต้องการทราบว่าผู้ใช้บริการเป็นผู้ใด กรณีที่ผู้ใช้บริการเคยลงทะเบียนและพิสูจน์ตัวตนกับ IdP ที่ RP เชื่อถือ RP จะนำผู้ใช้บริการ (redirect) ไปยังหน้าต่างยืนยันตัวตนของ IdP จากนั้นผู้ใช้บริการต้องยืนยันตัวตนด้วยการแสดงสิ่งที่ใช้ยืนยันตัวตนต่อ IdP เมื่อ IdP ตรวจสอบสิ่งที่ใช้ยืนยันตัวตนและสิ่งที่ใช้รับรองตัวตนเรียบร้อยแล้ว IdP จะส่งผลการยืนยันตัวตนให้กับ RP เพื่อให้ RP นำไปใช้พิจารณาอนุญาตให้ทำธุรกรรม หรือให้เข้าถึงข้อมูลหรือระบบต่อไป



รูปที่ 4 ตัวอย่างกระบวนการยืนยันตัวตน

RP และ IdP อาจเป็นหน่วยงานเดียวกันหรือต่างหน่วยงานกันก็ได้ กรณีที่ RP และ IdP ไม่ใช่หน่วยงานเดียวกัน RP ต้องเลือกใช้ข้อมูลจาก IdP ที่น่าเชื่อถือโดยพิจารณาจากวิธีการพิสูจน์ตัวตนและวิธีการยืนยันตัวตนที่ IdP ให้บริการกับผู้ใช้บริการ

IdP ต้องใช้เกณฑ์วิธียืนยันตัวตนที่สามารถรักษาความลับ (confidentiality) และความครบถ้วนสมบูรณ์ (integrity) ของข้อมูลที่รับ-ส่งระหว่างผู้ใช้บริการและ IdP ได้ นอกจากนี้ IdP ควรมีกลไกที่ใช้ป้องกันการโจมตีจากผู้ไม่ประสงค์ดี เช่น ระงับการใช้งานบัญชีผู้ใช้บริการเมื่อการยืนยันตัวตนของบัญชีนั้นผิดพลาดครบจำนวนครั้งที่กำหนด

4.4 การใช้งานดิจิทัลไอดีแบบกลุ่ม (Federation)

การใช้งานดิจิทัลไอดีแบบกลุ่ม (federation) หมายถึง การรวมกลุ่มของ IdP RP และ AS จากต่างระบบหรือต่างหน่วยงานเพื่อให้บริการยืนยันตัวตนกับผู้ใช้บริการด้วยดิจิทัลไอดี การใช้งานดิจิทัลไอดีในรูปแบบนี้มีประโยชน์หลายด้าน อาทิ

(1) เพิ่มความสะดวกให้กับผู้ใช้บริการ ซึ่งผู้ใช้บริการสามารถลงทะเบียนและพิสูจน์ตัวตนกับ IdP รายใดรายหนึ่ง ก็สามารถยืนยันตัวตนกับ IdP ดังกล่าวเพื่อเข้าใช้บริการหรือทำธุรกรรมกับ RP ที่อยู่ในกลุ่มเดียวกันได้

(2) ลดค่าใช้จ่ายด้านการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และโครงสร้างพื้นฐานด้านเทคโนโลยีของหน่วยงานที่เกี่ยวข้อง เนื่องจากหน่วยงานในกลุ่มเดียวกันสามารถใช้สิ่งที่ใช้ยืนยันตัวตนร่วมกันได้

(3) ทำให้ผู้ให้บริการสามารถมุ่งเน้นภารกิจที่เกี่ยวข้องโดยตรงกับการดำเนินธุรกิจ แทนที่ภารกิจด้านการบริหารจัดการไอเดนทิตี

รายละเอียดที่จะกล่าวต่อไปนี้ จะอธิบายส่วนประกอบของสถาปัตยกรรมการใช้งานดิจิทัลไอดีแบบกลุ่ม

4.4.1 ผลการยืนยันตัวตน (Assertion)

เมื่อเสร็จสิ้นกระบวนการยืนยันตัวตน IdP จะส่งผลการยืนยันตัวตนให้กับ RP โดยผลการยืนยันตัวตนประกอบด้วยผลการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน สิ่งที่ใช้รับรองตัวตน ไอเดนทิตี และคุณลักษณะของผู้ใช้บริการ (ถ้ามี)

IdP ต้องส่งผลการยืนยันตัวตนที่สร้างขึ้นไปยัง RP โดยตรง หากจำเป็นต้องส่งผลการยืนยันตัวตนจาก IdP ไปยัง RP ผ่านผู้ใช้บริการ IdP ต้องจัดให้มีกลไกรักษาความครบถ้วนสมบูรณ์ของผลการยืนยันตัวตนเพื่อไม่ให้มีการเปลี่ยนแปลงในภายหลัง

RP จะเชื่อถือผลการยืนยันตัวตนหรือไม่ขึ้นอยู่กับแหล่งที่มาของข้อมูล เวลาที่ผลการยืนยันตัวตนถูกสร้าง และนโยบายของ RP โดย RP ต้องตรวจสอบความครบถ้วนสมบูรณ์ (integrity) ของผลการยืนยันตัวตนเพื่อให้มั่นใจได้ว่าข้อมูลดังกล่าวไม่ถูกเปลี่ยนแปลงระหว่างการส่งมาจาก IdP ก่อนนำผลการยืนยันตัวตนไปใช้งาน

กรณีที่ผลการยืนยันตัวตนถูกส่งผ่านโครงข่ายสาธารณะ (public network) นั้น IdP ต้องมีวิธีการรักษาความลับของข้อมูลสำคัญ (sensitive information) ที่บรรจุอยู่ในผลการยืนยันตัวตนเพื่อให้เฉพาะ RP ที่กำหนดเท่านั้นสามารถเข้าถึงได้

4.4.2 การอนุญาตเฉพาะผู้มีสิทธิเข้าถึง (Authorization)

ในบางกรณี RP จำเป็นต้องเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้บริการที่เก็บอยู่ที่ AS หรือ IdP เพื่อนำข้อมูลดังกล่าวมาพิจารณากำหนดสิทธิของผู้ใช้บริการ เช่น กรณีที่ธนาคารต้องการเข้าถึงข้อมูลเครดิตของลูกค้าเพื่อให้สิทธิกู้ยืมเงิน การเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้บริการต้องได้รับการยินยอมจากผู้ใช้บริการก่อนทุกครั้ง และหลังจากเข้าถึงข้อมูลส่วนบุคคลแล้ว RP ต้องไม่นำข้อมูลส่วนบุคคลของผู้ใช้บริการไปกระทำการอื่นใดที่อยู่นอกเหนือขอบเขตที่ผู้ใช้บริการยินยอม

5. การบริหารความเสี่ยงของดิจิทัลไอดี

5.1 ภาพรวม

ความเสี่ยงของดิจิทัลไอดีตามข้อเสนอแนะมาตรฐานฉบับนี้ แบ่งออกเป็น 2 ด้าน คือ ความเสี่ยงของการพิสูจน์ตัวตนผิดพลาด เช่น ผู้สมัครใช้บริการแอบอ้างชื่อบุคคลอื่นในการลงทะเบียน และความเสี่ยงของการยืนยันตัวตนผิดพลาด เช่น ผู้แสดงสิ่งที่ใช้ยืนยันตัวตนไม่ใช่เจ้าของสิ่งที่ใช้ยืนยันตัวตน

วิธีการสำคัญในการบริหารความเสี่ยงดังกล่าวคือ การใช้วิธีการพิสูจน์ตัวตนและวิธีการยืนยันตัวตนที่มีความเข้มงวดสอดคล้องกับระดับผลกระทบที่สามารถเกิดขึ้นได้

5.2 ระดับความน่าเชื่อถือ

ระดับความน่าเชื่อถือบ่งบอกถึงความเข้มงวดของการพิสูจน์ตัวตนและการยืนยันตัวตน ซึ่งเป็นพื้นฐานในการพิจารณาระดับความมั่นใจของ RP ว่า (1) ไอเดนทิตีที่ผู้ใช้บริการกล่าวอ้างเป็นไอเดนทิตีของผู้ใช้บริการจริง เช่น ผู้ใช้บริการที่กล่าวอ้างว่าตนเองชื่อ “สมชาย” คือ สมชายตัวจริง ไม่ใช่บุคคลอื่นปลอมตัวมา และ (2) ผู้ใช้บริการเป็นเจ้าของสิ่งที่ใช้ยืนยันตัวตนจริง เช่น ผู้ที่กำลังเข้าใช้งานระบบ คือ สมชายตัวจริง ไม่ใช่

บุคคลอื่นขโมยรหัสผ่านไปใช้

หน่วยงานซึ่งทำหน้าที่เป็น RP ควรกำหนดระดับความน่าเชื่อถือ (assurance level) ของแต่ละบริการตามผลการประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ที่ให้บริการ ซึ่งข้อเสนอแนะมาตรฐานฉบับนี้ แบ่งระดับความน่าเชื่อถือเป็น 2 ด้าน ได้แก่

5.2.1 ระดับความน่าเชื่อถือของไอเดนทิตี (Identity Assurance Level: IAL)

ระดับความน่าเชื่อถือของไอเดนทิตี คือ ระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของผู้สมัครใช้บริการ การกำหนด IAL ที่เหมาะสมจะช่วยลดโอกาสของการพิสูจน์ตัวตนผิดพลาด โดย IAL แบ่งออกเป็น 3 ระดับ คือ

(1) ระดับ IAL1 ไม่มีข้อกำหนดในความเชื่อมโยงระหว่างตัวตนของผู้สมัครใช้บริการกับไอเดนทิตีที่มีอยู่ในโลกแห่งความจริง โดยคุณลักษณะใด ๆ ที่ใช้ลงทะเบียนเป็นคุณลักษณะที่ผู้สมัครใช้บริการยืนยันด้วยตนเอง (self-asserted) และไม่มีการตรวจสอบหรือพิสูจน์ความถูกต้องโดย IdP เช่น การสร้างบัญชีผู้ใช้งานอีเมล เป็นต้น

(2) ระดับ IAL2 กำหนดให้มีการพิจารณาหลักฐานแสดงตน โดย IdP ต้องตรวจสอบกับ AS ว่าไอเดนทิตีที่กล่าวอ้างมีอยู่ในโลกแห่งความจริง และตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง การพิสูจน์ตัวตนที่ระดับ IAL2 สามารถทำได้ทั้งแบบไม่พบเห็นต่อหน้า หรือแบบพบเห็นต่อหน้า

(3) ระดับ IAL3 เพิ่มความเข้มงวดให้กับข้อกำหนดที่ระดับ IAL2 ด้วยการพิจารณาหลักฐานแสดงตนเพิ่มเติม และการตรวจสอบข้อมูลชีวมิติ (biometric) เพื่อป้องกันการปลอมตัวเป็นบุคคลอื่น การหลอกลวง การลงทะเบียนซ้ำ หรือความเสียหายอื่น ๆ การพิสูจน์ตัวตนที่ระดับ IAL3 สามารถทำได้เฉพาะแบบพบเห็น ต่อหน้า ซึ่งรวมถึงแบบเสมือนพบเห็นต่อหน้าผ่านช่องทางอิเล็กทรอนิกส์

รายละเอียดของการลงทะเบียนและพิสูจน์ตัวตนสำหรับ IAL แต่ละระดับเป็นไปตามข้อเสนอแนะมาตรฐานฯ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การลงทะเบียนและพิสูจน์ตัวตน

5.2.2 ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level: AAL)

ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน คือ ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของผู้ใช้บริการ การกำหนด AAL ที่เหมาะสมจะช่วยลดโอกาสของการยืนยันตัวตนผิดพลาด เช่น ผู้ที่ยืนยันตัวตนไม่ใช่เจ้าของสิ่งที่ใช้ยืนยันตัวตน หรือไม่ใช่บุคคลที่ลงทะเบียนกับ IdP โดย AAL แบ่งออกเป็น 3 ระดับ คือ

(1) ระดับ AAL1: ใช้วิธีการยืนยันตัวตนแบบปัจจัยเดียว

(2) ระดับ AAL2: ใช้วิธีการยืนยันตัวตนแบบ 2 ปัจจัยที่ต่างกัน เช่น รหัสผ่าน (สิ่งที่ผู้ใช้บริการรู้) คู่กับ OTP (สิ่งที่ผู้ใช้บริการมี)

(3) ระดับ AAL3: ใช้วิธีการยืนยันตัวตนแบบ 2 ปัจจัยที่ต่างกัน และมีปัจจัยหนึ่งเป็นกุญแจเข้ารหัส (cryptographic key) เช่น USB Token ซึ่งบรรจุ private key ที่สามารถใช้งานได้เมื่อใส่รหัสผ่านถูกต้อง

รายละเอียดของการยืนยันตัวตนสำหรับ AAL แต่ละระดับเป็นไปตามข้อเสนอแนะมาตรฐานว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย – การยืนยันตัวตน

5.2.3 ข้อกำหนดของการเลือกระดับความน่าเชื่อถือของไอเดนทิตี และระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน

การเลือกระดับความน่าเชื่อถือของไอเดนทิตี (IAL) กับระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL) แยกจากกันทำให้เกิดความยืนหยุ่นในการพัฒนาระบบให้บริการของหน่วยงาน อย่างไรก็ตาม มีข้อจำกัดสำหรับการใช้ IAL และ AAL บางระดับร่วมกัน เนื่องจากข้อมูลส่วนบุคคลที่ผู้ใช้บริการใช้ลงทะเบียนกับ IdP และสิ่งที่ใช้ยืนยันตัวตนที่จะป้องกันการเข้าถึงข้อมูลดังกล่าวจากบุคคลที่ไม่ได้รับอนุญาตต้องมีความสอดคล้องกัน ดังนั้น การจัดกลุ่ม IAL และ AAL ที่สามารถใช้งานร่วมกันได้เป็นไปตามตารางที่ 1

ตารางที่ 1 ระดับ IAL และ AAL ที่สามารถใช้งานร่วมกันได้

	AAL1	AAL2	AAL3
IAL1: ไม่มีข้อมูลส่วนบุคคล	สามารถใช้ได้	สามารถใช้ได้	สามารถใช้ได้
IAL1: มีข้อมูลส่วนบุคคล	ไม่สามารถใช้ได้	สามารถใช้ได้	สามารถใช้ได้
IAL2	ไม่สามารถใช้ได้	สามารถใช้ได้	สามารถใช้ได้
IAL3	ไม่สามารถใช้ได้	สามารถใช้ได้	สามารถใช้ได้

5.3 การกำหนดระดับความน่าเชื่อถือ

วิธีการกำหนดระดับความน่าเชื่อถือของแต่ละหน่วยงานอาจมีความแตกต่างกันขึ้นอยู่กับมาตรฐานหรือกรอบการดำเนินงาน (framework) ที่ใช้อ้างอิง ตัวอย่างเช่น มาตรฐาน ISO/IEC 29115:2013 กำหนดระดับความน่าเชื่อถือ 4 ระดับจากระดับ 1 (สำหรับความน่าเชื่อถือต่ำที่สุด) และระดับ 4 (สำหรับความน่าเชื่อถือสูงที่สุด) ในขณะที่มาตรฐาน NIST 800-63-3 ของสหรัฐอเมริกากำหนดความน่าเชื่อถือเป็น 3 ระดับจากระดับ 1 (สำหรับความน่าเชื่อถือต่ำที่สุด) และระดับ 3 (สำหรับความน่าเชื่อถือสูงที่สุด)

การใช้งานดิจิทัลไอดีสำหรับประเทศไทยกำหนดให้มีการแบ่งระดับความน่าเชื่อถือออกเป็น 2 ด้าน คือ ความน่าเชื่อถือของไอเดนทิตี (IAL) และความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL) โดยแต่ละด้านมี 3 ระดับ การกำหนดระดับความน่าเชื่อถือของไอเดนทิตี (IAL) และความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL) ให้เหมาะสมกับการให้บริการนั้น RP ควรดำเนินการ 2 ขั้นตอน คือ

ขั้นตอนที่ 1 ประเมินระดับผลกระทบที่เป็นไปได้ (เมื่อการพิสูจน์ตัวตนผิดพลาด สำหรับกำหนด IAL และเมื่อการยืนยันตัวตนผิดพลาด สำหรับกำหนด AAL)

ขั้นตอนที่ 2 เชื่อมโยงผลการประเมินระดับผลกระทบที่เป็นไปได้กับระดับความน่าเชื่อถือ

5.3.1 ขั้นตอนที่ 1 ประเมินระดับผลกระทบที่เป็นไปได้

การประเมินระดับผลกระทบที่เป็นไปได้ (potential impacts) เป็นการพิจารณาผลกระทบที่เป็นไปได้จากข้อผิดพลาดในการพิสูจน์ตัวตน (สำหรับกำหนดระดับ IAL) และผลกระทบที่เป็นไปได้จากข้อผิดพลาดในการยืนยันตัวตน (สำหรับกำหนดระดับ AAL)

ข้อเสนอแนะมาตรฐานฉบับนี้แบ่งประเภทของผลกระทบเป็น 6 ด้าน ประกอบด้วย ความไม่สะดวกสบายและเสื่อมเสียชื่อเสียง ความเสียหายทางการเงิน ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ความปลอดภัย

ของบุคคล และการละเมิดกฎหมายแพ่งหรืออาญา [1][3] ทั้งนี้ RP อาจเพิ่มเติมประเภทของกระทบอื่น ๆ ให้สอดคล้องกับความเป็นจริงได้ โดยอ้างอิงจากนโยบายด้านความเสี่ยงของหน่วยงาน

การประเมินระดับผลกระทบที่เป็นไปได้ จะใช้วิธีการพิจารณาระดับผลกระทบแต่ละด้านที่สามารถเกิดขึ้นได้เมื่อมีข้อผิดพลาดโดยมีรายละเอียดตามตารางที่ 2

ตารางที่ 2 เกณฑ์การพิจารณาระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด

ด้านของผลกระทบ	ระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด		
	ต่ำ	ปานกลาง	สูง
ความไม่สะดวกสบายและเสื่อมเสียชื่อเสียง	อย่างรุนแรงที่สุดคือ มีความไม่สะดวกสบายและเสื่อมเสียชื่อเสียงในระยะสั้น และจำกัด	อย่างรุนแรงที่สุดคือ มีความไม่สะดวกสบายและเสื่อมเสียชื่อเสียงรุนแรง ระยะสั้น หรือมีผลปานกลางในระยะยาว	มีความไม่สะดวกสบายและเสื่อมเสียชื่อเสียงระยะยาว หรือมีผลกระทบหลายบุคคล
ความเสียหายทางการเงิน	อย่างรุนแรงที่สุดคือ มีความเสียหายทางการเงินที่ไม่มีนัยสำคัญ	อย่างรุนแรงที่สุดคือ มีความเสียหายทางการเงินรุนแรง	มีความเสียหายทางการเงินรุนแรงมาก
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	อย่างรุนแรงที่สุดคือ มีผลกระทบที่จำกัดต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	อย่างรุนแรงที่สุดคือ มีผลกระทบรุนแรงต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	มีผลกระทบรุนแรงมากต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	อย่างรุนแรงที่สุดคือ มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับต่ำ	อย่างรุนแรงที่สุดคือ มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับปานกลาง	มีการปล่อยข้อมูลส่วนบุคคล หรือข้อมูลสำคัญทางการค้าให้กับผู้ไม่ได้รับอนุญาต ทำให้ความลับที่เปิดเผยมีผลกระทบระดับสูง
ความปลอดภัยของบุคคล	อย่างรุนแรงที่สุดคือ บาดเจ็บเล็กน้อย ไม่ต้องรับการรักษาพยาบาล	อย่างรุนแรงที่สุดคือ มีความเสี่ยงพอสมควรที่จะบาดเจ็บเล็กน้อย หรือมีความเสี่ยงจำกัดที่จะบาดเจ็บซึ่งต้องการการรักษาพยาบาล	มีความเสี่ยงที่จะบาดเจ็บสาหัส หรือถึงแก่ชีวิต

ด้านของผลกระทบ	ระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาด		
	ต่ำ	ปานกลาง	สูง
การละเมิดทางแพ่งหรือทางอาญา	อย่างรุนแรงที่สุดคือการฝ่าฝืนกฎหมายนั้นเป็นเรื่องเล็กน้อย ซึ่งไม่จำเป็นต้องมีการบังคับใช้กฎหมาย	อย่างรุนแรงที่สุดคือการฝ่าฝืนกฎหมายนั้นมีความเสี่ยงที่จะถูกบังคับใช้กฎหมาย	การฝ่าฝืนกฎหมายนั้นมีความเสี่ยงสูงเป็นพิเศษในการที่จะถูกบังคับใช้กฎหมาย

5.3.2 ขั้นตอนที่ 2 เชื่อมโยงผลการประเมินระดับผลกระทบที่เป็นไปได้กับระดับความน่าเชื่อถือ

ผลการประเมินระดับผลกระทบที่เป็นไปได้เมื่อเกิดข้อผิดพลาดในการพิสูจน์ตัวตนและการยืนยันตัวตนจากขั้นตอนที่ 1 จะถูกนำมาใช้พิจารณาระดับความน่าเชื่อถือ IAL และ AAL ตามลำดับ โดยระดับความน่าเชื่อถือที่เหมาะสมคือระดับที่ครอบคลุมผลกระทบที่เป็นไปได้ทุกด้าน ตามตารางที่ 3

ตารางที่ 3 ผลกระทบที่เป็นไปได้และระดับความน่าเชื่อถือที่ต้องการ

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

5.3.3 ตัวอย่างการกำหนดระดับความน่าเชื่อถือ

ตัวอย่างการกำหนดระดับความน่าเชื่อถือของไอเดนทิตี (IAL): และระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL) ของผู้ให้บริการออนไลน์รายหนึ่ง มีขั้นตอนดังนี้

(1) การกำหนดระดับความน่าเชื่อถือของไอเดนทิตี (IAL):

ขั้นตอนที่ 1 ประเมินระดับผลกระทบที่เป็นไปได้จากข้อผิดพลาดในการพิสูจน์ตัวตนผู้สมัครใช้บริการ โดยมีตัวอย่างผลการประเมินดังนี้

ด้านของผลกระทบ	ผลการประเมินระดับผลกระทบ
ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง	ต่ำ
ความเสียหายทางการเงิน	ต่ำ

ด้านของผลกระทบ	ผลการประเมินระดับผลกระทบ
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	ไม่มี
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	ไม่มี
ความปลอดภัยของบุคคล	ไม่มี
การละเมิดทางแพ่งหรือทางอาญา	ไม่มี

ขั้นตอนที่ 2 เชื่อมโยงผลการประเมินระดับผลกระทบที่เป็นไปได้จากขั้นตอนที่ 1 กับระดับความน่าเชื่อถือ

ด้านของผลกระทบ	ระดับความน่าเชื่อถือ		
	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

จากการเชื่อมโยงผลการประเมินระดับผลกระทบที่เป็นไปได้เข้ากับระดับความน่าเชื่อถือ เห็นได้ว่าระดับความน่าเชื่อถือที่ครอบคลุมผลกระทบที่เป็นไปได้ในทุกด้านคือระดับ 1 ดังนั้น ระดับความน่าเชื่อถือของไอเดนทิตีที่เหมาะสมกับบริการนี้คือ 1 (ระดับ IAL1)

(2) การกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (AAL):

ขั้นตอนที่ 1 ประเมินระดับผลกระทบที่เป็นไปได้จากข้อผิดพลาดในการยืนยันตัวตนของผู้ใช้บริการ โดยมีตัวอย่างการประเมินดังนี้

ด้านของผลกระทบ	ผลการประเมินระดับผลกระทบ
ความไม่สะดวกสบาย และเสื่อมเสียชื่อเสียง	ต่ำ
ความเสียหายทางการเงิน	ต่ำ
ความเสียหายต่อการดำเนินงานขององค์กรหรือต่อผลประโยชน์สาธารณะ	ต่ำ

ด้านของผลกระทบ	ผลการประเมินระดับผลกระทบ
การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต	ปานกลาง
ความปลอดภัยของบุคคล	ไม่มี
การละเมิดทางแพ่งหรือทางอาญา	ต่ำ

ขั้นตอนที่ 2 เชื่อมโยงผลการประเมินระดับผลกระทบที่เป็นไปได้จากขั้นตอนที่ 1 กับระดับความน่าเชื่อถือ

ด้านของผลกระทบ	ระดับความน่าเชื่อถือ		
	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

จากการเชื่อมโยงผลการประเมินระดับผลกระทบที่เป็นไปได้เข้ากับระดับความน่าเชื่อถือ เห็นได้ว่าระดับความน่าเชื่อถือที่ครอบคลุมผลกระทบที่เป็นไปได้ในทุกด้านคือระดับ 2 ดังนั้น ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนที่เหมาะสมกับบริการนี้คือ 2 (ระดับ AAL2)

บรรณานุกรม

[1] NIST Special Publication 800-63-3, "Digital Identity Guidelines", June 2017.
Available: https://doi.org/10.6028/NIST.SP.800-63-3

[2] World Bank Group, GSMA, and Secure Identity Alliance, "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation", 2016.

[3] ISO/IEC 29115:2013, "Information technology - Security techniques - Entity authentication assurance framwork"