(ร่าง) **มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์**

ว่าด้วย

การพิสูจน์และยืนยันตัวตนทางดิจิทัล

(Digital Identity)

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

ที่มาและความสำคัญ

สพธอ. และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชนจึงได้ร่วมกันจัดทำมาตรฐานแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย โดยประกาศเป็น **ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ (ETDA Recommendation)** เมื่อ**วันที่ 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 **กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์**กำหนดให้บุคคลสามารถพิสูจน์และยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ โดยมี**กลไกการควบคุมดูแลผู้ประกอบธุรกิจบริการที่เกี่ยวข้อง**เพื่อให้ระบบดังกล่าวมีความน่าเชื่อถือและปลอดภัย ป้องกันความเสียหายที่อาจเกิดขึ้นต่อสาธารณชน ตลอดจน**เสริมสร้างความน่าเชื่อถือและการยอมรับในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล**

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้พิจารณาแก้ไขปรับปรุงข้อเสนอแนะมาตรฐานฯ ฉบับเดิม เพื่อให้แนวทางการพิสูจน์และยืนยันตัวตนทางดิจิทัล มีความสอดคล้องกับบริบทการใช้งาน ความต้องการทางธุรกิจ และคุณลักษณะของระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลในประเทศไทย โดยกำหนดเป็น**มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล** เพื่อมา**ใช้แทนข้อเสนอแนะมาตรฐานฯ ฉบับเดิม** และ**ยกเลิกข้อเสนอแนะมาตรฐานฯ ฉบับเดิม** (ขมธอ. 18-2561 ขมธอ. 19-2561 และ ขมธอ. 20-2561)

มาตรฐาน การพิสูจน์และยืนยันตัวตนทางดิจิทัล จำนวน 3 ฉบับ

1 **เล่ม 1 กรอบการทำงาน (Part 1: Framework)**

เป็นเอกสารอธิบาย**คำศัพท์ กระบวนการ การประเมินความเสี่ยง และการกำหนดระดับความน่าเชื่อถือ**ที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อให้ผู้ที่เกี่ยวข้องกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความเข้าใจตรงกัน

2 **เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน (Part 2: Identity Proofing Requirements)**

เป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ใน**การพิสูจน์ตัวตนของบุคคลที่ประสงค์จะใช้บริการหรือทำธุรกรรมออนไลน์** เพื่อให้ IdP มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกันตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)

3 **เล่ม 3 ข้อกำหนดของการยืนยันตัวตน (Part 3: Authentication Requirements)**

เป็นข้อกำหนดสำหรับผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) ใน**การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนและการยืนยันตัวตนของผู้ใช้บริการผ่านทางออนไลน์** เพื่อให้ IdP มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกันตามระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL)

เล่ม 1 กรอบการทำงาน (Part 1: Framework)

เป็นเอกสารอธิบาย

- **คำศัพท์**
- **กระบวนการ**
- **การประเมินความเสี่ยง และ**
- **การกำหนดระดับความน่าเชื่อถือ**

ที่เกี่ยวข้องกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่อให้ผู้ที่เกี่ยวข้องกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลมีความเข้าใจตรงกัน

โครงสร้างของเอกสาร

1. ขอบข่าย

2. บทนิยาม

3. การพิสูจน์และยืนยันตัวตนทางดิจิทัล

3.1 ภาพรวม

3.2 ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้อง

3.3 สิ่งที่ใช้ยืนยันตัวตน

3.4 ผลการยืนยันตัวตน

3.5 ดิจิทัลไอดีแบบรวมกลุ่ม (Federated Identity)

4. การกำหนดระดับความน่าเชื่อถือ

4.1 ภาพรวม

4.2 ระดับความน่าเชื่อถือ

4.3 การประเมินความเสี่ยงเพื่อกำหนดระดับความน่าเชื่อถือ

4.4 ตัวอย่างการกำหนดระดับความน่าเชื่อถือ

ภาคผนวก ก. อักษรย่อ

บรรณานุกรม

สรุปประเด็นที่มีการปรับปรุงจาก ขมธอ. 18-2561

ขมธอ. 18-2561 ภาพรวมและอภิธานศัพท์	(ร่าง) มธอ. เล่ม 1 กรอบการทำงาน
1. ขอบข่าย	**1. ขอบข่าย**
2. บทนิยาม	**2. บทนิยาม**
2.1 คุณลักษณะ (attribute) หมายถึง ลักษณะ (characteristic) หรือคุณสมบัติ (property) ของบุคคล	ปรับนิยามเป็น **2.2 คุณลักษณะ (identity attribute)** หมายถึง ข้อมูลที่เกี่ยวข้องกับบุคคล ตัวอย่างเช่น เลขประจำตัว ชื่อบุคคล วันเดือนปีเกิด ที่อยู่อีเมล หมายเลขโทรศัพท์เคลื่อนที่ หรือข้อมูลระบุอุปกรณ์ที่บุคคลใช้งาน
2.2 ไอเดนทิตี (identity หรือ ID) หมายถึง คุณลักษณะ หรือชุดของคุณลักษณะที่ใช้ระบุตัวบุคคลในบริบทที่กำหนด	ปรับนิยามเป็น **2.3 อัตลักษณ์ (identity)** หมายถึง คุณลักษณะหรือชุดของคุณลักษณะที่เกี่ยวข้องกับตัวบุคคล ซึ่งเป็นลักษณะเฉพาะและสามารถบ่งบอกหรือจำแนกบุคคลได้ภายในบริบทที่กำหนด [ร่าง พ.ร.ฎ.]
2.3 ดิจิทัลไอดี (digital identity หรือ digital ID) หมายถึง คุณลักษณะ หรือชุดของคุณลักษณะที่ถูกรวบรวมและบันทึกในรูปแบบดิจิทัล ซึ่งสามารถใช้ระบุตัวบุคคลในบริบทที่กำหนด และสามารถใช้ทำธุรกรรมอิเล็กทรอนิกส์	ลบนิยาม เนื่องจากเอกสารจะใช้คำว่า “อัตลักษณ์ (identity)” เป็นหลัก แต่มีคำอธิบายไว้ใน 3.1 ภาพรวม ว่า ดิจิทัลไอดี (digital identity) คือ อัตลักษณ์ (identity) ของบุคคล ซึ่งใช้บ่งบอกหรือจำแนกบุคคลในการทำธุรกรรมออนไลน์
2.4 สิ่งที่ใช้ยืนยันตัวตน (authenticator) หมายถึง สิ่งที่ผู้ใช้บริการครอบครองเพื่อใช้ในการยืนยันตัวตน โดยสิ่งที่ใช้ยืนยันตัวตนจะมีปัจจัยของการยืนยันตัวตนอย่างน้อยหนึ่งปัจจัย	ปรับนิยามเป็น **2.5 สิ่งที่ใช้ยืนยันตัวตน (authenticator)** หมายถึง สิ่งที่บุคคลเป็นเจ้าของหรือครอบครองเพื่อใช้ในการยืนยันอัตลักษณ์ของบุคคล โดยสิ่งที่ใช้ยืนยันตัวตนทุกอันจะมีปัจจัยของการยืนยันตัวตน (authentication factor) อย่างน้อยหนึ่งปัจจัย ได้แก่ สิ่งที่คุณรู้ (something you know) สิ่งที่คุณมี (something you have) และสิ่งที่คุณเป็น (something you are)
2.5 สิ่งที่ใช้รับรองตัวตน (credential) หมายถึง เอกสาร วัตถุ (object) หรือกลุ่มข้อมูล (data structure) ที่เชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตน ตัวอย่างเช่น หนังสือเดินทาง บัตรประจำตัวประชาชน หรือ ใบรับรองอิเล็กทรอนิกส์ (digital certificate)	ลบนิยามและเนื้อหาที่เกี่ยวข้อง เนื่องจากเป็นเพียงการขยายความจาก “สิ่งที่ใช้ยืนยันตัวตน (authenticator)” และไม่จำเป็นต้องกล่าวถึงใน เล่ม 3 ข้อกำหนดของการยืนยันตัวตน

สรุปประเด็นที่มีการปรับปรุงจาก ขมธอ. 18-2561

ขมธอ. 18-2561 ภาพรวมและอภิธานศัพท์	(ร่าง) มธอ. เล่ม 1 กรอบการทำงาน
2.6 ผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP) หมายถึง บุคคลหรือหน่วยงานที่น่าเชื่อถือซึ่งทำหน้าที่ (1) รับลงทะเบียน (enrolment) และพิสูจน์ตัวตน (identity proofing) และ (2) บริหารจัดการสิ่งที่ใช้รับรองตัวตน (credential) ซึ่งเชื่อมโยงไอเดนทิตีเข้ากับสิ่งที่ใช้ยืนยันตัวตน (authenticator) ของผู้ใช้บริการ โดยผู้พิสูจน์และยืนยันตัวตนอาจบริหารจัดการสิ่งที่ใช้รับรองตัวตนเพื่อใช้ภายในองค์กรหรือใช้ภายนอกองค์กรก็ได้	ปรับนิยามเป็น **2.9 ผู้พิสูจน์และยืนยันตัวตน (identity provider: IdP)** หมายถึง หน่วยงานที่ให้บริการการพิสูจน์ตัวตน การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน และการยืนยันตัวตน ทั้งนี้ IdP อาจออกสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ภายในกิจการของหน่วยงานหรือให้บริการแก่บุคคลภายนอกก็ได้
2.7 ผู้ให้บริการ (relying party: RP) หมายถึง บุคคลหรือหน่วยงานซึ่งให้บริการทำธุรกรรม หรืออนุญาตให้เข้าถึงข้อมูลหรือระบบ โดยอาศัย (1) สิ่งที่ใช้ยืนยันตัวตน (authenticator) และ (2) ผลการยืนยันตัวตน (assertion) หรือสิ่งที่ใช้รับรองตัวตน (credential) จากผู้พิสูจน์และยืนยันตัวตน	ปรับนิยามเป็น **2.10 ผู้อาศัยการยืนยันตัวตน (relying party: RP)** หมายถึง บุคคลหรือหน่วยงานที่พึ่งพาอาศัยผลการยืนยันตัวตนจาก IdP หรือสิ่งที่ใช้ยืนยันตัวตนที่ผู้ใช้บริการมีอยู่ก่อนแล้ว ในการตัดสินใจที่จะให้บริการธุรกรรมหรือให้สิทธิในการเข้าใช้งานระบบ
2.8 ผู้ให้ข้อมูลที่น่าเชื่อถือ (authoritative source: AS) หมายถึง บุคคลหรือหน่วยงานที่มีความน่าเชื่อถือและสามารถเข้าถึงหรือมีข้อมูลที่ถูกต้อง และทำหน้าที่ (1) ตรวจสอบข้อมูลหรือสถานะของหลักฐานแสดงตนของผู้ใช้บริการตามการร้องขอจากผู้พิสูจน์และยืนยันตัวตน หรือ (2) อนุญาตให้ผู้ให้บริการเข้าถึงข้อมูลที่น่าเชื่อถือ หรือข้อมูลส่วนบุคคลซึ่งได้รับความยินยอมจากผู้ใช้บริการ	ปรับนิยามเป็น **2.11 แหล่งข้อมูลที่น่าเชื่อถือ (authoritative source: AS)** หมายถึง หน่วยงานที่มีการให้หรือจัดทำข้อมูลเกี่ยวกับอัตลักษณ์ที่ถูกต้อง เพื่อให้ IdP สามารถใช้ตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลหรือตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์ได้
2.9 ผู้สมัครใช้บริการ (applicant) หมายถึง บุคคลที่สมัครใช้บริการพิสูจน์และยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน	ลบนิยาม เนื่องจาก ใช้คำว่า “บุคคล” แทน จึงไม่ต้องมีนิยาม
2.10 ผู้ใช้บริการ (subscriber) หมายถึง ผู้สมัครใช้บริการที่ผ่านการลงทะเบียนและพิสูจน์ตัวตนกับผู้พิสูจน์และยืนยันตัวตน และได้รับสิ่งที่ใช้ยืนยันตัวตนสำหรับใช้ยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตน	ปรับนิยามเป็น **2.12 ผู้ใช้บริการ (subscriber)** หมายถึง บุคคลที่ผ่านการพิสูจน์ตัวตนและได้รับสิ่งที่ใช้ยืนยันตัวตนเพื่อใช้ในการยืนยันตัวตน

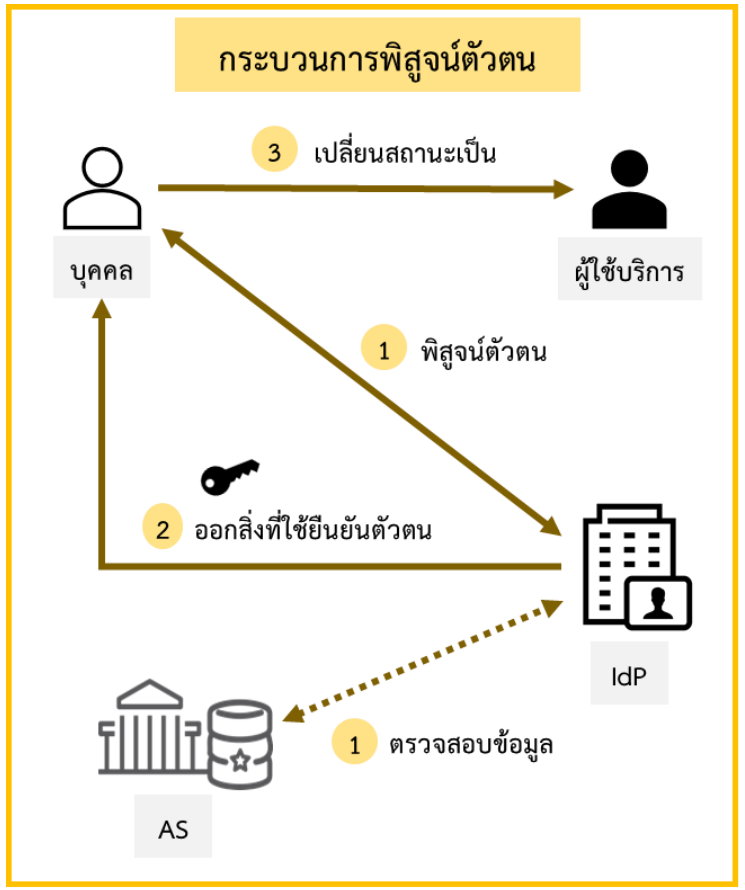
สรุปประเด็นที่มีการปรับปรุงจาก ขมธอ. 18-2561

ขมธอ. 18-2561 ภาพรวมและอภิธานศัพท์	(ร่าง) มธอ. เล่ม 1 กรอบการทำงาน
2.11 การลงทะเบียน (enrolment) หมายถึง กระบวนการที่ผู้สมัครใช้บริการลงทะเบียนเป็นผู้ใช้บริการของผู้พิสูจน์และยืนยันตัวตน	ลบนิยาม เนื่องจากเป็นกระบวนการเดียวกันกับ “การพิสูจน์ตัวตน” และทำให้เกิดความสงสัยว่าบุคคลต้องลงทะเบียนกับ Platform เพิ่มเติมจากการลงทะเบียนกับ IdP ด้วยหรือไม่
2.12 การพิสูจน์ตัวตน (identity proofing) หมายถึง กระบวนการที่ผู้พิสูจน์และยืนยันตัวตนรวบรวมข้อมูล ตรวจสอบหลักฐานแสดงตน และตรวจสอบตัวตนของผู้สมัครใช้บริการ	ปรับนิยามเป็น **2.6 การพิสูจน์ตัวตน (identity proofing)** หมายถึง กระบวนการรวบรวมและตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคล และการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับอัตลักษณ์นั้น [ร่าง พ.ร.ฎ.]
2.13 การยืนยันตัวตน (authentication) หมายถึง กระบวนการที่ผู้ใช้บริการยืนยันตัวตนกับผู้พิสูจน์และยืนยันตัวตนว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้างด้วยการใช้สิ่งที่ใช้ยืนยันตัวตน (authenticator)	ปรับนิยามเป็น **2.8 การยืนยันตัวตน (authentication)** หมายถึง กระบวนการตรวจสอบสิ่งที่ใช้ยืนยันตัวตนเพื่อยืนยันอัตลักษณ์ของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตนนั้น [ร่าง พ.ร.ฎ.]
2.14 การอนุญาตเฉพาะผู้มีสิทธิเข้าถึง (authorization) หมายถึง กระบวนการที่ผู้ใช้บริการอนุญาตให้ผู้ให้บริการเข้าถึงข้อมูลของตน	ลบนิยามและเนื้อหาที่เกี่ยวข้อง เนื่องจากเป็นกระบวนการภายหลังการยืนยันตัวตนสำเร็จ และไม่อยู่ในขอบข่ายของมาตรฐาน
	เพิ่มนิยาม **2.1 การพิสูจน์และยืนยันตัวตน** หมายถึง กระบวนการพิสูจน์และยืนยันความถูกต้องของตัวบุคคล [พ.ร.บ.]
	เพิ่มนิยาม **2.4 หลักฐานแสดงตน (identity evidence หรือ identity document)** หมายถึง เอกสารทางกายภาพหรือข้อมูลอิเล็กทรอนิกส์ ซึ่งสามารถใช้เป็นหลักฐานในการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคล
	เพิ่มนิยาม **2.7 การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน (authenticator management)** หมายถึง กระบวนการเชื่อมโยงอัตลักษณ์ของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้ยืนยันตัวตน และการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนนั้น [ร่าง พ.ร.ฎ.]
	เพิ่มนิยาม **2.13 ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)** หมายถึง ระดับความมั่นใจหรือระดับความเข้มงวดในกระบวนการพิสูจน์ตัวตนของบุคคล
	เพิ่มนิยาม **2.14 ระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL)** หมายถึง ระดับความมั่นใจหรือระดับความเข้มงวดในกระบวนการยืนยันตัวตนของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตน

3.2 ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้อง

กระบวนการพิสูจน์ตัวตน

1) บุคคลมาแสดงตนกับ IdP ซึ่ง **IdP จะพิสูจน์ตัวตนของบุคคลตามระดับ IAL** ที่กำหนด โดยอาจมีการตรวจสอบหลักฐานแสดงตนและข้อมูลเกี่ยวกับอัตลักษณ์กับ AS
2) หากการพิสูจน์ตัวตนสำเร็จ **IdP จะออกหรือลงทะเบียนสิ่งที่ใช้ยืนยันตัวตน** และเชื่อมโยงอัตลักษณ์ของบุคคลเข้ากับสิ่งที่ใช้ยืนยันตัวตนนั้น
3) บุคคลที่ผ่านการพิสูจน์ตัวตนแล้วจะเปลี่ยนสถานะเป็น **ผู้ใช้บริการ** และมีหน้าที่ดูแลรักษาสิ่งที่ใช้ยืนยันตัวตน



IdP คือ ผู้พิสูจน์และยืนยันตัวตน (identity provider)
RP คือ ผู้อาศัยการยืนยันตัวตน (relying party)
AS คือ แหล่งข้อมูลที่น่าเชื่อถือ (authoritative source)

กระบวนการยืนยันตัวตน

1) ผู้ใช้บริการขอทำธุรกรรมออนไลน์กับ RP โดยใช้**ดิจิทัลไอดีที่มีระดับ IAL และ AAL สอดคล้องตามความต้องการของ RP**
2) RP นำทาง (redirect) ผู้ใช้บริการไปยังหน้าต่างยืนยันตัวตนของ IdP และให้**ผู้ใช้บริการยืนยันตัวตนกับ IdP ตามเกณฑ์วิธีหรือระดับ AAL** ที่กำหนด
3) IdP ตรวจสอบความถูกต้องและสถานะของสิ่งที่ใช้ยืนยันตัวตน แล้ว**ส่งผลการยืนยันตัวตนให้กับ RP** ซึ่ง RP สามารถใช้ข้อมูลจากผลการยืนยันตัวตนในการตัดสินใจที่จะให้บริการธุรกรรมกับผู้ใช้บริการ
4) **RP ทำการเชื่อมต่อกับผู้ใช้บริการ**เพื่อให้บริการธุรกรรมออนไลน์

สรุปประเด็นที่มีการปรับปรุงจาก ขมธอ. 18-2561

ขมธอ. 18-2561 ภาพรวมและอภิธานศัพท์	(ร่าง) มธอ. เล่ม 1 กรอบการทำงาน
3. อักษรย่อ	ย้ายหัวข้อเป็น **ภาคผนวก ก. อักษรย่อ**
4. แบบจำลองดิจิทัลไอดี (Digital ID Model)	ปรับหัวข้อเป็น **3. การพิสูจน์และยืนยันตัวตนทางดิจิทัล**
4.1 ภาพรวม	ปรับหัวข้อเป็น **3.1 ภาพรวม** และ **3.2 ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้อง**
4.2 การลงทะเบียนและพิสูจน์ตัวตน	ลบหัวข้อ เนื่องจากเป็นการขยายความจาก **3.2 ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้อง** และซ้ำซ้อนกับ **เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน**
4.3 การยืนยันตัวตน	ลบหัวข้อ แต่ไม่ลบเนื้อหาในหัวข้อย่อย
4.3.1 สิ่งที่ใช้ยืนยันตัวตน	**3.3 สิ่งที่ใช้ยืนยันตัวตน**
4.3.2 สิ่งที่ใช้รับรองตัวตน	ลบหัวข้อ เนื่องจากเป็นเพียงการขยายความจาก “สิ่งที่ใช้ยืนยันตัวตน (authenticator)” และไม่จำเป็นต้องกล่าวถึงใน เล่ม 3 ข้อกำหนดของการยืนยันตัวตน
4.3.3 กระบวนการยืนยันตัวตน	ลบหัวข้อ เนื่องจากเป็นการขยายความจาก **3.2 ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้อง**
4.4 การใช้งานดิจิทัลไอดีแบบกลุ่ม (Federation)	ปรับหัวข้อเป็น **3.5 ดิจิทัลไอดีแบบ Federated Identity**
4.4.1 ผลการยืนยันตัวตน (Assertion)	**3.4 ผลการยืนยันตัวตน**
4.4.2 การอนุญาตเฉพาะผู้มีสิทธิเข้าถึง (Authorization)	ลบหัวข้อ เนื่องจากเป็นกระบวนการภายหลังการยืนยันตัวตนสำเร็จ และไม่อยู่ในขอบข่ายของมาตรฐาน

สรุปประเด็นที่มีการปรับปรุงจาก ขมธอ. 18-2561

ขมธอ. 18-2561 ภาพรวมและอภิธานศัพท์	(ร่าง) มธอ. เล่ม 1 กรอบการทำงาน
5. การบริหารความเสี่ยงของดิจิทัลไอดี	ปรับหัวข้อเป็น **4. การกำหนดระดับความน่าเชื่อถือ** เนื่องจากการประเมินความเสี่ยงมีวัตถุประสงค์เพื่อกำหนดระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (IAL) และระดับความน่าเชื่อถือของการยืนยันตัวตน (AAL)
5.1 ภาพรวม	**4.1 ภาพรวม**
5.2 ระดับความน่าเชื่อถือ	**4.2 ระดับความน่าเชื่อถือ**
5.2.1 ระดับความน่าเชื่อถือของไอเดนทิตี (Identity Assurance Level: IAL)	ปรับคำของ IAL เป็น (1) ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL) และลบเนื้อหา คำอธิบายของ IAL เนื่องจากซ้ำซ้อนกับ เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน
5.2.2 ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level: AAL)	ปรับคำของ AAL เป็น (2) ระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance Level: AAL) และลบเนื้อหา คำอธิบายของ AAL เนื่องจากซ้ำซ้อนกับ เล่ม 3 ข้อกำหนดของการยืนยันตัวตน
5.2.3 ข้อกำหนดของการเลือกระดับความน่าเชื่อถือของไอเดนทิตี และระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน	ลบเนื้อหา เนื่องจากเป็นเนื้อหาที่เฉพาะเจาะจงกับกฎหมาย Executive Order ของสหรัฐอเมริกา ซึ่งกำหนดให้ใช้ Multi-factor Authentication (MFA) กับการให้ข้อมูลส่วนบุคคล
5.3 การกำหนดระดับความน่าเชื่อถือ	ปรับหัวข้อเป็น **4.3 การประเมินความเสี่ยงเพื่อกำหนดระดับความน่าเชื่อถือ**
5.3.1 ขั้นตอนที่ 1 ประเมินระดับผลกระทบที่เป็นไปได้	ปรับหัวข้อเป็น (1) ขั้นตอนที่ 1: การประเมินระดับผลกระทบที่เป็นไปได้
5.3.2 ขั้นตอนที่ 2 เชื่อมโยงผลการประเมินระดับผลกระทบที่เป็นไปได้กับระดับความน่าเชื่อถือ	ปรับหัวข้อเป็น (2) ขั้นตอนที่ 2: การเชื่อมโยงระดับผลกระทบที่เป็นไปได้เข้ากับระดับความน่าเชื่อถือ
5.3.3 ตัวอย่างการกำหนดระดับความน่าเชื่อถือ	**4.4 ตัวอย่างการกำหนดระดับความน่าเชื่อถือ**

เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน (Part 2: Identity Proofing Requirements)

เป็นข้อกำหนดสำหรับ IdP ใน**การพิสูจน์ตัวตนของบุคคลที่ประสงค์จะใช้บริการหรือทำธุรกรรมออนไลน์**
เพื่อให้ IdP มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกันตามระดับความน่าเชื่อถือของการพิสูจน์ตัวตน **(identity assurance level: IAL)**

โครงสร้างของเอกสาร

1. ขอบข่าย

2. การพิสูจน์ตัวตน

- 2.1 การแยกแยะตัวตน
- 2.2 การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์
- 2.3 การตรวจสอบตัวบุคคล

3. ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL)

- 3.1 ระดับ IAL1
- 3.2 ระดับ IAL2
- 3.3 ระดับ IAL3

4. ข้อกำหนดของการพิสูจน์ตัวตน

- 4.1 ข้อกำหนดของการแยกแยะตัวตน
- 4.2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์
  - 4.2.1 ประเภทของหลักฐานแสดงตนและวิธีการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์
  - 4.2.2 การอาศัยผลการยืนยันจาก IdP ที่เคยพิสูจน์ตัวตนมาก่อน
- 4.3 ข้อกำหนดของการตรวจสอบตัวบุคคล
  - 4.3.1 ข้อกำหนดของการเปรียบเทียบข้อมูลชีวมิติ
- 4.4 สรุปข้อกำหนดที่สำคัญของการพิสูจน์ตัวตนตามระดับ IAL

บรรณานุกรม

สรุปประเด็นที่มีการปรับปรุงจาก ขมธอ. 19-2561

ขมธอ. 19-2561 การลงทะเบียนและพิสูจน์ตัวตน	(ร่าง) มธอ. เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน
1. ขอบข่าย	**1. ขอบข่าย**
2. ระดับความน่าเชื่อถือของไอเดนทิตี (Identity Assurance Level)	ปรับคำของ IAL และหัวข้อเป็น **3. ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (Identity Assurance Level: IAL)**
2.1 ระดับ IAL1	**3.1 ระดับ IAL1**
2.2 ระดับ IAL2 “ระดับ IAL2 กำหนดให้มีการพิจารณาหลักฐานแสดงตน โดย IdP ต้องตรวจสอบกับ AS ว่าไอเดนทิตีที่กล่าวอ้างมีอยู่ในโลกแห่งความจริง และตรวจสอบผู้สมัครใช้บริการว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง การพิสูจน์ตัวตนที่ระดับ IAL2 สามารถทำได้ทั้งแบบไม่พบเห็นต่อหน้า หรือแบบพบเห็นต่อหน้า”	**3.2 ระดับ IAL2** และปรับคำอธิบายให้ชัดเจนขึ้นเป็น “ระดับ IAL2 กำหนดให้มีการขอหลักฐานแสดงตน การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ว่าอัตลักษณ์ที่กล่าวอ้างมีอยู่ในโลกแห่งความเป็นจริง และการตรวจสอบความเชื่อมโยงระหว่างอัตลักษณ์นั้นกับบุคคลจริงที่แสดงตน ทั้งนี้ การพิสูจน์ตัวตนที่ระดับ IAL2 สามารถทำได้ทั้งแบบพบเห็นต่อหน้า หรือแบบไม่พบเห็นต่อหน้า เช่น การพิสูจน์ตัวตนผ่านเครื่องให้บริการ (kiosk) หรือแอปพลิเคชันของ IdP”
2.3 ระดับ IAL3 “ระดับ IAL3 เพิ่มความเข้มงวดให้กับข้อกำหนดที่ระดับ IAL2 ด้วยการพิจารณาหลักฐานแสดงตนเพิ่มเติมและการตรวจสอบข้อมูลชีวมิติ (biometric) เพื่อป้องกันการปลอมตัวเป็นบุคคลอื่น การหลอกลวง การลงทะเบียนซ้ำ หรือความเสียหายอื่นๆ การพิสูจน์ตัวตนที่ระดับ IAL3 สามารถทำได้เฉพาะแบบพบเห็นต่อหน้า ซึ่งรวมถึงแบบเสมือนพบเห็นต่อหน้าผ่านช่องทางอิเล็กทรอนิกส์”	**3.3 ระดับ IAL3** และปรับคำอธิบายให้ชัดเจนขึ้นเป็น “ระดับ IAL3 เพิ่มความเข้มงวดจากระดับ IAL2 โดยกำหนดให้มีการขอหลักฐานแสดงตนเพิ่มเติม และการตรวจสอบความเชื่อมโยงระหว่างอัตลักษณ์ที่กล่าวอ้างกับบุคคลจริงที่แสดงตนโดยการเปรียบเทียบข้อมูลชีวมิติ (biometric comparison) เพื่อป้องกันการปลอมตัวเป็นบุคคลอื่นและการลงทะเบียนซ้ำ ทั้งนี้ การพิสูจน์ตัวตนที่ระดับ IAL3 สามารถทำได้แบบพบเห็นต่อหน้าเท่านั้น”

สรุปประเด็นที่มีการปรับปรุงจาก ขมธอ. 19-2561

ขมธอ. 19-2561 การลงทะเบียนและพิสูจน์ตัวตน	(ร่าง) มธอ. เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน
3. การลงทะเบียนและพิสูจน์ตัวตน	ปรับหัวข้อเป็น **2. การพิสูจน์ตัวตน**
3.1 การระบุตัวตน “การระบุตัวตน เป็นกระบวนการที่ IdP รวบรวมคุณลักษณะและหลักฐานแสดงตนที่จำเป็นจากผู้สมัครใช้บริการ เพื่อแยกแยะว่าไอเดนทิตีของผู้สมัครใช้บริการมีเพียงหนึ่งเดียวและมีความเฉพาะเจาะจงภายในบริบทหรือกลุ่มผู้ใช้บริการที่กำหนด ทั้งนี้ การระบุตัวตนที่ดีควรใช้ชุดของคุณลักษณะเท่าที่จำเป็นในการแยกแยะไอเดนทิตีของผู้สมัครใช้บริการแต่ละราย”	ปรับหัวข้อเป็น **2.1 การแยกแยะตัวตน** และปรับคำอธิบายให้ชัดเจนขึ้นเป็น “การแยกแยะตัวตน (identity resolution) คือ กระบวนการที่ IdP รวบรวมหลักฐานแสดงตนและข้อมูลเกี่ยวกับอัตลักษณ์จากบุคคลที่สมัครใช้บริการ เพื่อใช้แยกแยะว่าอัตลักษณ์ของบุคคลที่สมัครใช้บริการมีเพียงอันเดียวและมีความเฉพาะเจาะจงภายในบริบทของบริการธุรกรรม”
3.2 การตรวจสอบหลักฐานแสดงตน “การตรวจสอบหลักฐานแสดงตน เป็นกระบวนการที่ IdP ตรวจสอบความแท้จริง (authenticity) สถานะการใช้งาน (validity) และความถูกต้อง (accuracy) ของหลักฐานแสดงตน และตรวจสอบข้อมูลที่อยู่ในหลักฐานแสดงตนว่าเป็นของบุคคลที่มีตัวตนอยู่จริง รวมถึงตรวจสอบช่องทางการติดต่อว่าสามารถใช้ติดต่อได้”	ปรับหัวข้อเป็น **2.2 การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์** และปรับคำอธิบายให้ชัดเจนขึ้นเป็น “การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ (identity validation) คือ กระบวนการที่ IdP ตรวจสอบความถูกต้อง ความแท้จริง และความเป็นปัจจุบันของข้อมูลเกี่ยวกับอัตลักษณ์ เพื่อพิสูจน์ว่าอัตลักษณ์ที่กล่าวอ้างมีอยู่ในโลกแห่งความเป็นจริง”
3.3 การตรวจสอบตัวบุคคล “การตรวจสอบตัวบุคคล เป็นกระบวนการที่ IdP ตรวจสอบตัวบุคคลที่แสดงหลักฐานแสดงตนว่าเป็นเจ้าของไอเดนทิตีที่กล่าวอ้าง”	**2.3 การตรวจสอบตัวบุคคล** และปรับคำอธิบายให้ชัดเจนขึ้นเป็น “การตรวจสอบตัวบุคคล (identity verification) คือ กระบวนการที่ IdP ตรวจสอบความเชื่อมโยงระหว่างอัตลักษณ์ที่กล่าวอ้างกับบุคคลจริงที่แสดงตน เพื่อพิสูจน์ว่าอัตลักษณ์ที่กล่าวอ้างเป็นอัตลักษณ์จริงของบุคคลที่กำลังพิสูจน์ตัวตนกับ IdP”

สรุปประเด็นที่มีการปรับปรุงจาก ขมธอ. 19-2561

ขมธอ. 19-2561 การลงทะเบียนและพิสูจน์ตัวตน	(ร่าง) มธอ. เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน
4. ข้อกำหนดเกี่ยวกับการลงทะเบียนและพิสูจน์ตัวตน	ปรับหัวข้อเป็น **4. ข้อกำหนดของการพิสูจน์ตัวตน**
4.1 ข้อกำหนดทั่วไป (ที่ระดับ IAL2 และ IAL3)	ลบหัวข้อ เนื่องจากเนื้อหาส่วนนี้จะไปเป็นส่วนหนึ่งในประกาศหลักเกณฑ์การประกอบธุรกิจของ IdP
4.2 ข้อกำหนดของการแสดงตน	ลบหัวข้อ และย้ายเนื้อหาไปรวมไว้ใน **4.3 ข้อกำหนดของการตรวจสอบตัวบุคคล**
4.2.1 ข้อกำหนดของการพิสูจน์ตัวตนแบบพบเห็นต่อหน้า (ที่ระดับ IAL3)	ลบหัวข้อ และย้ายเนื้อหาไปรวมไว้ใน **4.3 ข้อกำหนดของการตรวจสอบตัวบุคคล**
4.2.2 ข้อกำหนดของการพิสูจน์ตัวตนแบบเสมือนพบเห็นต่อหน้าผ่านช่องทางอิเล็กทรอนิกส์ (ที่ระดับ IAL3)	ลบหัวข้อ เนื่องจาก Live VDO conference ที่ kiosk ยังไม่มีการใช้งานในบริบทของประเทศไทย
4.3 ข้อกำหนดของการระบุตัวตน	ปรับหัวข้อเป็น **4.1 ข้อกำหนดของการแยกแยะตัวตน** และปรับคำอธิบาย – IAL1 ปรับเป็น IdP อาจรวบรวมข้อมูลเกี่ยวกับอัตลักษณ์ ซึ่งเป็นคุณลักษณะที่บุคคลยืนยันด้วยตนเอง (self-asserted) – IAL2 / IAL3 ย้าย การขอหลักฐานแสดงตน มาอยู่ในหัวข้อ 4.1 ข้อกำหนดของการแยกแยะตัวตน นี้ – IAL2 / IAL3 ลบเนื้อหา IdP อาจใช้วิธีการที่เหมาะสมในการพิจารณาความแตกต่างของข้อมูลส่วนบุคคล และ IdP อาจใช้ knowledge-based verification (KBV) เนื่องจากบริบทของประเทศไทยมีการแยกแยะตัวตนด้วยเลขประจำตัวประชาชน

สรุปประเด็นที่มีการปรับปรุงจาก ขมธอ. 19-2561

ขมธอ. 19-2561 การลงทะเบียนและพิสูจน์ตัวตน	(ร่าง) มธอ. เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน
4.4 ข้อกำหนดของการตรวจสอบหลักฐานแสดงตน	ปรับหัวข้อเป็น **4.2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์** และปรับคำอธิบาย – IAL1 มีการยกตัวอย่างการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์ด้วยวิธีการอื่น ๆ ที่ไม่สอดคล้องตาม IAL2 ทั้งนี้ IAL1 จะไม่มีการแบ่งระดับย่อยเป็น IAL1.1 / IAL1.2 / IAL1.3 เนื่องจากการตรวจสอบด้วยวิธีการอื่น ๆ ที่ไม่สอดคล้องตาม IAL2 จะถือว่าเป็นคุณลักษณะที่บุคคลยืนยันด้วยตนเอง (self-asserted) ซึ่งไม่ได้รับการตรวจสอบความถูกต้อง และไม่อยู่ภายใต้การกำกับดูแล – IAL2 / IAL3 กำหนดวิธีการตรวจสอบความถูกต้องและความแท้จริงของข้อมูล ไว้ในหัวข้อย่อยใหม่ คือ หัวข้อ 4.2.1 – IAL2 / IAL3 การตรวจสอบความเป็นปัจจุบันของข้อมูลเกี่ยวกับอัตลักษณ์ด้วยระบบการตรวจสอบของหน่วยงานของรัฐ เพิ่มวิธีการให้รองรับ “ผลการยืนยันตัวตนจาก IdP ที่เคยดำเนินการมาก่อน”
	เพิ่มหัวข้อย่อย **4.2.1 ประเภทของหลักฐานแสดงตนและวิธีการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์** เพื่อกำหนดประเภทของหลักฐานแสดงตนและวิธีการตรวจสอบที่นำมาใช้ โดยเพิ่มวิธีการให้รองรับ “หลักฐานแสดงตนในรูปของข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือ ซึ่งออกโดยหน่วยงานของรัฐ” และ “ผลการยืนยันตัวตนจาก IdP ที่เคยดำเนินการมาก่อน”
	เพิ่มหัวข้อย่อย **4.2.2 การอาศัยผลการยืนยันจาก IdP ที่เคยพิสูจน์ตัวตนมาก่อน** เพื่ออธิบายเพิ่มเติม
4.5 ข้อกำหนดของการตรวจสอบตัวบุคคล	**4.3 ข้อกำหนดของการตรวจสอบตัวบุคคล** โดยเพิ่มวิธีการให้รองรับ “การเปรียบเทียบข้อมูลชีวมิติของบุคคลด้วยระบบการตรวจสอบของหน่วยงานของรัฐ” และ “การอาศัยผลการยืนยันตัวตนจาก IdP ที่เคยเปรียบเทียบข้อมูลชีวมิติของบุคคลมาก่อน”
	เพิ่มหัวข้อย่อย **4.3.1 ข้อกำหนดของการเปรียบเทียบข้อมูลชีวมิติ** เพื่อกำหนด FMR ไม่เกิน 0.1% และ FNMR ไม่เกิน 3% รวมถึงข้อกำหนดอื่น ๆ ของการเปรียบเทียบข้อมูลชีวมิติ
4.6 ข้อกำหนดของการตรวจสอบช่องทางการติดต่อ	ลบหัวข้อ และย้ายเนื้อหาไปรวมไว้ใน **4.2 ข้อกำหนดของการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์**

4.2.1 ประเภทของหลักฐานแสดงตนและวิธีการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์

ประเภทของหลักฐานแสดงตน	วิธีการตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์
กรณีของบุคคลที่มีสัญชาติไทย	
(1) บัตรประจำตัวประชาชนแบบอเนกประสงค์ (smart card)	การตรวจสอบกับข้อมูลที่อ่านจากเครื่องอ่านบัตรประจำตัวประชาชนแบบอเนกประสงค์
(2) หนังสือเดินทางของประเทศไทย และเอกสารสำคัญประจำตัวอื่นที่ออกโดยหน่วยงานของรัฐ	การตรวจสอบกับข้อมูลที่อ่านจากชิปของหนังสือเดินทางด้วยเทคโนโลยีสื่อสารไร้สายระยะใกล้ (NFC) และตรวจสอบเอกสารสำคัญประจำตัวอื่นที่ออกโดยหน่วยงานของรัฐ (เช่น ทะเบียนบ้าน ใบขับขี่)
(3) หลักฐานแสดงตนในรูปของข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือซึ่งออกโดยหน่วยงานของรัฐ	การตรวจสอบหลักฐานแสดงตนในรูปของข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือด้วยระบบการตรวจสอบของหน่วยงานของรัฐหรือด้วยกระบวนการเข้ารหัสลับ
(4) ผลการยืนยันตัวตนจาก IdP ที่เคยตรวจสอบความถูกต้องและความแท้จริงของข้อมูลเกี่ยวกับอัตลักษณ์	การอาศัยข้อมูลเกี่ยวกับอัตลักษณ์จากผลการยืนยันตัวตนที่ส่งให้โดย IdP ที่เคยตรวจสอบความถูกต้องและความแท้จริงของข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลมาก่อน
กรณีของคนต่างด้าว	
(1) หนังสือเดินทางของต่างประเทศ และเอกสารสำคัญประจำตัวอื่นที่รัฐบาลไทยออกให้หรือหน่วยงานของรัฐเจ้าของสัญชาติออกให้	การตรวจสอบกับข้อมูลที่อ่านจากชิปของหนังสือเดินทางด้วยเทคโนโลยีสื่อสารไร้สายระยะใกล้ (NFC) และตรวจสอบเอกสารสำคัญประจำตัวอื่นที่รัฐบาลไทยออกให้หรือหน่วยงานของรัฐเจ้าของสัญชาติออกให้ (เช่น วีซ่า ใบอนุญาตทำงาน)
(2) หลักฐานแสดงตนในรูปของข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือซึ่งออกโดยหน่วยงานของรัฐ	การตรวจสอบหลักฐานแสดงตนในรูปของข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือด้วยระบบการตรวจสอบของหน่วยงานของรัฐหรือด้วยกระบวนการเข้ารหัสลับ
(3) ผลการยืนยันตัวตนจาก IdP ที่เคยตรวจสอบความถูกต้องและความแท้จริงของข้อมูลเกี่ยวกับอัตลักษณ์	การอาศัยข้อมูลเกี่ยวกับอัตลักษณ์จากผลการยืนยันตัวตนที่ส่งให้โดย IdP ที่เคยตรวจสอบความถูกต้องและความแท้จริงของข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลมาก่อน

สรุปประเด็นที่มีการปรับปรุงจาก ขมธอ. 19-2561

ขมธอ. 19-2561 การลงทะเบียนและพิสูจน์ตัวตน	(ร่าง) มธอ. เล่ม 2 ข้อกำหนดของการพิสูจน์ตัวตน
4.7 สรุปข้อกำหนดตามระดับ IAL	ปรับหัวข้อเป็น **4.4 สรุปข้อกำหนดที่สำคัญของการพิสูจน์ตัวตนตามระดับ IAL** และปรับคำอธิบายเป็นตาราง Checklist ที่แยกระหว่าง “การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า” และ ”การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า” และในวิธีการปฏิบัติ IAL2 จะแบ่งออกเป็น 3 ระดับย่อย คือ IAL2.1 / IAL2.2 / IAL2.3 โดยพิจารณาจากการตรวจสอบความเป็นปัจจุบันของข้อมูลเกี่ยวกับอัตลักษณ์ และวิธีการที่ IdP ใช้ในการตรวจสอบตัวบุคคล
5. แนวทางการกำหนดระดับ IAL ของประเทศไทย	

ระดับความน่าเชื่อถือของการพิสูจน์ตัวตน (identity assurance level: IAL)

ข้อกำหนดของการพิสูจน์ตัวตน	การพิสูจน์ตัวตนแบบไม่พบเห็นต่อหน้า					การพิสูจน์ตัวตนแบบพบเห็นต่อหน้า				
	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3	IAL1	IAL2.1	IAL2.2	IAL2.3	IAL3
การแยกแยะตัวตน										
ขอหลักฐานแสดงตน จำนวน 1 อันจากตัวเลือกที่กำหนด		✓	✓	✓			✓	✓	✓	
ขอหลักฐานแสดงตน จำนวน 2 อันจากตัวเลือกที่กำหนด										✓
รวบรวมข้อมูลเกี่ยวกับอัตลักษณ์เพื่อใช้แยกแยะว่าอัตลักษณ์มีเพียงอันเดียวและมีความเฉพาะเจาะจงภายในบริบทของบริการธุรกรรม		✓	✓	✓			✓	✓	✓	✓
การตรวจสอบข้อมูลเกี่ยวกับอัตลักษณ์										
ตรวจสอบความถูกต้องและความแท้จริงของข้อมูลเกี่ยวกับอัตลักษณ์จากหลักฐานแสดงตน โดยใช้วิธีการที่กำหนด ดังนี้ (1) การตรวจสอบกับข้อมูลที่อ่านจากเครื่องอ่านบัตรประจำตัวประชาชนแบบอเนกประสงค์ (2) การตรวจสอบกับข้อมูลที่อ่านจากชิปของหนังสือเดินทางด้วยเทคโนโลยีสื่อสารไร้สายระยะใกล้ (NFC) และตรวจสอบเอกสารสำคัญประจำตัวอื่นที่รัฐบาลไทยออกให้หรือหน่วยงานของรัฐเจ้าของสัญชาติออกให้ (3) การตรวจสอบหลักฐานแสดงตนในรูปของข้อมูลอิเล็กทรอนิกส์ที่น่าเชื่อถือด้วยระบบการตรวจสอบของหน่วยงานของรัฐ หรือด้วยกระบวนการเข้ารหัสลับ (4) การอาศัยข้อมูลเกี่ยวกับอัตลักษณ์จากผลการยืนยันตัวตนที่ส่งให้โดย IdP ที่เคยตรวจสอบความถูกต้องและความแท้จริงของข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลมาก่อน		✓	✓	✓			✓	✓	✓	✓
ตรวจสอบความเป็นปัจจุบันของข้อมูลเกี่ยวกับอัตลักษณ์ด้วยระบบการตรวจสอบของหน่วยงานของรัฐ หรืออาศัยผลการยืนยันตัวตนจาก IdP ที่เคยตรวจสอบความเป็นปัจจุบันของข้อมูลเกี่ยวกับอัตลักษณ์ด้วยระบบการตรวจสอบของหน่วยงานของรัฐมาก่อนไม่เกิน 1 ปี			✓	✓				✓	✓	✓
ยืนยันช่องทางการติดต่อของบุคคลที่สมัครใช้บริการ เช่น การยืนยัน OTP ที่ส่งให้ทางอีเมลหรือหมายเลขโทรศัพท์		✓ (ควร)	✓ (ควร)	✓ (ควร)			✓ (ควร)	✓ (ควร)	✓ (ควร)	✓ (ควร)
การตรวจสอบตัวบุคคล										
ให้เจ้าหน้าที่เปรียบเทียบลักษณะใบหน้าหรือภาพใบหน้าของบุคคลกับภาพของบุคคลจากหลักฐานแสดงตน (visual comparison)		✓	✓				✓	✓		
ใช้วิธีการใดวิธีการหนึ่ง ดังนี้ (1) การใช้เทคโนโลยีเปรียบเทียบภาพใบหน้าของบุคคลกับข้อมูลชีวมิติจากหลักฐานแสดงตน (biometric comparison) (2) การเปรียบเทียบข้อมูลชีวมิติของบุคคลด้วยระบบการตรวจสอบของหน่วยงานของรัฐ (3) การอาศัยผลการยืนยันตัวตนจาก IdP ที่เคยเปรียบเทียบข้อมูลชีวมิติของบุคคลมาก่อน				✓					✓	✓
มีเทคโนโลยีการตรวจจับการปลอมแปลงชีวมิติ (presentation attack detection) เช่น การตรวจจับการมีชีวิตของบุคคล (liveness detection)				✓						
บันทึกข้อมูลชีวมิติตั้งต้นของบุคคล (biometric sample) เพื่อป้องกันการปฏิเสธว่าไม่ได้พิสูจน์ตัวตนหรือเพื่อใช้พิสูจน์ตัวตนอีกครั้ง										✓

เล่ม 3 ข้อกำหนดของการยืนยันตัวตน (Part 3: Authentication Requirements)

เป็นข้อกำหนดสำหรับ IdP ใน**การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนและการยืนยันตัวตนของผู้ใช้บริการผ่านทางออนไลน์**
เพื่อให้ IdP มีแนวปฏิบัติที่เป็นมาตรฐานเดียวกันตามระดับความน่าเชื่อถือของการยืนยันตัวตน **(authentication assurance level: AAL)**

โครงสร้างของเอกสาร

1. ขอบข่าย

2. ระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level)

2.1 ระดับ AAL1

2.2 ระดับ AAL2

2.3 ระดับ AAL3

2.4 สรุปข้อกำหนดที่สำคัญของการยืนยันตัวตนตามระดับ AAL

2.5 ข้อสังเกตสำหรับการยืนยันตัวตนแบบพบเห็นต่อหน้า

3. ข้อกำหนดตามชนิดของสิ่งที่ใช้ยืนยันตัวตน

3.1 รหัสลับจดจำ (memorized secret)

3.2 อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device)

3.3 อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device)

3.4 อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device)

3.5 ซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software)

3.6 อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic device)

3.7 ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic software)

3.8 อุปกรณ์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic device)

4. ข้อกำหนดทั่วไปของสิ่งที่ใช้ยืนยันตัวตน

4.1 สิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์

4.2 การจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาด

4.3 การใช้งานชีวมิติ

4.4 การป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)

4.5 การป้องกัน IdP ตัวปลอม (IdP-impersonation resistance)

5. การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน

5.1 การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน

5.2 การสูญหาย ถูกขโมย เสียหาย และการออกทดแทน

5.3 การหมดอายุและการออกใหม่

5.4 การเพิกถอน

6. การบริหารจัดการเซสชัน

6.1 การผูกเซสชัน (session binding)

6.2 การยืนยันตัวตนซ้ำ (reauthentication)

บรรณานุกรม

ระดับความน่าเชื่อถือของการยืนยันตัวตน (authentication assurance level: AAL)

AAL1 กำหนดให้ใช้การยืนยันตัวตนแบบปัจจัยเดียว (single-factor authentication) เป็นอย่างน้อย ด้วย authentication protocol ที่มั่นคงปลอดภัย

AAL2 กำหนดให้ใช้การยืนยันตัวตนด้วยปัจจัยของการยืนยันตัวตนที่แตกต่างกัน 2 ปัจจัยเป็นอย่างน้อย ด้วย authentication protocol ที่มั่นคงปลอดภัย

AAL3 กำหนดให้ใช้การยืนยันตัวตนด้วยปัจจัยของการยืนยันตัวตนที่แตกต่างกัน 2 ปัจจัยเป็นอย่างน้อย และใช้สิ่งที่ใช้ยืนยันตัวตนที่มีคุณสมบัติ (1) เป็นฮาร์ดแวร์ (hardware-based) (2) บรรจุกุญแจเข้ารหัส (cryptographic key) และ (3) สามารถป้องกัน IdP ตัวปลอม (IdP-impersonation resistance)

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

สรุปประเด็นที่มีการปรับปรุงจาก ขมธอ. 20-2561

ขมธอ. 20-2561 การยืนยันตัวตน	(ร่าง) มธอ. เล่ม 3 ข้อกำหนดของการยืนยันตัวตน
1. ขอบข่าย	**1. ขอบข่าย**
2. ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level)	ปรับคำของ AAL เป็น **2. ระดับความน่าเชื่อถือของการยืนยันตัวตน (Authentication Assurance Level)**
2.1 ระดับ AAL1	**2.1 ระดับ AAL1**
2.1.1 ข้อกำหนดเกี่ยวกับชนิดของสิ่งที่ใช้ยืนยันตัวตน	ปรับหัวข้อเป็น “ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้”
2.1.2 ข้อกำหนดทั่วไป	ปรับหัวข้อเป็น “ข้อกำหนดที่สำคัญ” และลบข้อกำหนด “การยืนยันตัวตนซ้ำ (reauthentication)” เนื่องจากการบริหารจัดการเซสชันเป็น optional โดยอธิบายอยู่แล้วใน 6.2 การยืนยันตัวตนซ้ำ (reauthentication)
2.2 ระดับ AAL2	**2.2 ระดับ AAL2**
2.2.1 ข้อกำหนดเกี่ยวกับชนิดของสิ่งที่ใช้ยืนยันตัวตน	ปรับหัวข้อเป็น “ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้” และลบตัวเลือก memorized secret + SF crypto device เนื่องจากซ้ำซ้อนกับ Authenticator ใน AAL3
2.2.2 ข้อกำหนดทั่วไป	ปรับหัวข้อเป็น “ข้อกำหนดที่สำคัญ” และลบข้อกำหนด “การยืนยันตัวตนซ้ำ (reauthentication)” ตามเหตุผลข้างต้น และลบข้อกำหนด “การใช้งานชีวมิติ” เนื่องจากสิ่งที่ใช้ยืนยันตัวตนบางชนิดไม่มีชีวมิติ อย่างไรก็ตาม อธิบายอยู่แล้วใน 4.3 การใช้งานชีวมิติ
2.3 ระดับ AAL3	**2.3 ระดับ AAL3**
2.3.1 ข้อกำหนดเกี่ยวกับชนิดของสิ่งที่ใช้ยืนยันตัวตน	ปรับหัวข้อเป็น “ชนิดของสิ่งที่ใช้ยืนยันตัวตนที่สามารถใช้ได้”
2.3.2 ข้อกำหนดทั่วไป	ปรับหัวข้อเป็น “ข้อกำหนดที่สำคัญ” และลบข้อกำหนด “การยืนยันตัวตนซ้ำ (reauthentication)” และ “การใช้งานชีวมิติ” ตามเหตุผลข้างต้น
	เพิ่มหัวข้อ **2.5 ข้อสังเกตสำหรับการยืนยันตัวตนแบบพบเห็นต่อหน้า** เพื่ออธิบายว่าการยืนยันตัวตนผ่านทางออนไลน์มีความแตกต่างกับการยืนยันตัวตนแบบพบเห็นต่อหน้า

สรุปประเด็นที่มีการปรับปรุงจาก ขมธอ. 20-2561

ขมธอ. 20-2561 การยืนยันตัวตน	(ร่าง) มธอ. เล่ม 3 ข้อกำหนดของการยืนยันตัวตน
3. ชนิดและข้อกำหนดสิ่งที่ใช้ยืนยันตัวตน	ปรับหัวข้อเป็น **3. ข้อกำหนดตามชนิดของสิ่งที่ใช้ยืนยันตัวตน**
3.1 ชนิดของสิ่งที่ใช้ยืนยันตัวตน	ลบหัวข้อ 3.1 ชนิดของสิ่งที่ใช้ยืนยันตัวตน และ 3.2 ข้อกำหนดทั่วไปของสิ่งที่ใช้ยืนยันตัวตน โดยแยกเนื้อหาเป็น 2 บท คือ **3. ข้อกำหนดตามชนิดของสิ่งที่ใช้ยืนยันตัวตน** และ **4. ข้อกำหนดทั่วไปของสิ่งที่ใช้ยืนยันตัวตน**
3.1.1 รหัสลับจดจำ (memorized secret)	**3.1 รหัสลับจดจำ (memorized secret)**
3.1.2 อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device)	**3.2 อุปกรณ์สื่อสารช่องทางอื่น (out-of-band device)**
3.1.3 อุปกรณ์ OTP ปัจจัยเดียว (single-factor OTP device)	**3.3 อุปกรณ์ OTP แบบปัจจัยเดียว (single-factor OTP device)** และลบข้อกำหนด “ช่องทางที่มีความปลอดภัยเพื่อป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance)” เนื่องจากมีอยู่แล้วในข้อกำหนดที่สำคัญ ของหัวข้อ 2.1 ระดับ AAL1 / 2.2 ระดับ AAL2 / 2.3 ระดับ AAL3
3.1.4 อุปกรณ์ OTP หลายปัจจัย (multi-factor OTP device)	**3.4 อุปกรณ์ OTP แบบหลายปัจจัย (multi-factor OTP device)** และลบข้อกำหนด “ช่องทางที่มีความปลอดภัยเพื่อป้องกันการโจมตีโดยคนกลาง (man-in-the-middle resistance)” ตามเหตุผลข้างต้น
3.1.5 ซอฟต์แวร์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic software)	**3.5 ซอฟต์แวร์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic software)**
3.1.6 อุปกรณ์เข้ารหัสลับปัจจัยเดียว (single-factor cryptographic device)	**3.6 อุปกรณ์เข้ารหัสลับแบบปัจจัยเดียว (single-factor cryptographic device)**
3.1.7 ซอฟต์แวร์เข้ารหัสลับหลายปัจจัย (multi-factor cryptographic software)	**3.7 ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic software)**
3.1.8 อุปกรณ์เข้ารหัสลับหลายปัจจัย (multi-factor cryptographic devices)	**3.8 อุปกรณ์เข้ารหัสลับแบบหลายปัจจัย (multi-factor cryptographic device)**

สรุปประเด็นที่มีการปรับปรุงจาก ขมธอ. 20-2561

ขมธอ. 20-2561 การยืนยันตัวตน	(ร่าง) มธอ. เล่ม 3 ข้อกำหนดของการยืนยันตัวตน
3.2 ข้อกำหนดทั่วไปของสิ่งที่ใช้ยืนยันตัวตน	**4. ข้อกำหนดทั่วไปของสิ่งที่ใช้ยืนยันตัวตน**
3.2.1 สิ่งที่ใช้ยืนยันตัวตนที่เป็นวัตถุ	ปรับหัวข้อเป็น **4.1 สิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์**
3.2.2 การจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาด	**4.2 การจำกัดจำนวนครั้งของการยืนยันตัวตนผิดพลาด**
3.2.3 การใช้งานชีวมิติ (biometric)	**4.3 การใช้งานชีวมิติ** และเพิ่มข้อกำหนด “เทคโนโลยีการตรวจจับการปลอมแปลงชีวมิติต้องมีผลการทดสอบเป็นไปตามมาตรฐาน ISO/IEC 30107-3 Information technology – Biometric presentation attack detection – Part 3: Testing and reporting ที่ระดับ Evaluation Assurance Level 1 เป็นอย่างน้อย”
	เพิ่มหัวข้อ **4.4 การป้องกันการโจมตีแบบส่งข้อมูลซ้ำ (replay resistance)**
	เพิ่มหัวข้อ **4.5 การป้องกัน IdP ตัวปลอม (IdP-impersonation resistance)**
4. การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน	**5. การบริหารจัดการสิ่งที่ใช้ยืนยันตัวตน**
4.1 การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน (authenticator binding)	**5.1 การเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตน** และเพิ่มข้อกำหนด เกี่ยวกับการเชื่อมโยงสิ่งที่ใช้ยืนยันตัวตนเพิ่มเติมหรือสิ่งที่ใช้ยืนยันตัวตนที่ผู้ใช้บริการมีอยู่ก่อนแล้วเข้ากับบัญชีของผู้ใช้บริการ
4.2 การสูญหาย ถูกโจรกรรม และเสียหายของสิ่งที่ใช้ยืนยันตัวตน	ปรับหัวข้อเป็น **5.2 การสูญหาย ถูกขโมย เสียหาย และการออกทดแทน** และเพิ่มข้อกำหนดของการออกทดแทน
4.3 การหมดอายุ	ปรับหัวข้อเป็น **5.3 การหมดอายุและการออกใหม่** และเพิ่มข้อกำหนดของการออกใหม่
4.4 การเพิกถอน	**5.4 การเพิกถอน**

สรุปประเด็นที่มีการปรับปรุงจาก ขมธอ. 20-2561

ขมธอ. 20-2561 การยืนยันตัวตน	(ร่าง) มธอ. เล่ม 3 ข้อกำหนดของการยืนยันตัวตน
5. การบริหารจัดการ session	ปรับหัวข้อเป็น **6. การบริหารจัดการเซสชัน** และอธิบายให้ชัดเจนว่า “IdP อาจกำหนดระยะเวลาของเซสชัน (session)” หรือ optional
5.1 ข้อกำหนดทั่วไป	ปรับหัวข้อเป็น **6.1 การผูกเซสชัน (session binding)**
5.2 กลไกบริหารจัดการ session (session management mechanism)	ลบหัวข้อและเนื้อหา แต่อธิบายเพิ่มเติมว่า ตัวอย่างของวิธีการบริหารจัดการ session (เช่น cookies ของเว็บเบราว์เซอร์) สามารถอ้างอิงเพิ่มเติมจากเอกสาร Session Management Cheat Sheet ของ Open Web Application Security Project (OWASP)
5.2.1 cookies	
5.2.2 access token	
5.2.3 การระบุอุปกรณ์ (device identification)	
5.3 การยืนยันตัวตนซ้ำ (reauthentication)	**6.2 การยืนยันตัวตนซ้ำ (reauthentication)** และเพิ่มข้อกำหนดของการยืนยันตัวตนซ้ำ ให้ชัดเจน
6. แนวทางการกำหนดระดับ AAL ของประเทศไทย	ย้ายหัวข้อเป็น **2.4 สรุปข้อกำหนดที่สำคัญของการยืนยันตัวตนตามระดับ AAL** และลบระดับ AAL2.2 (และเปลี่ยน AAL2.1 เป็น AAL2 ปกติ) เนื่องจากชีวมิติไม่ถือเป็นข้อมูลลับ จึงไม่เป็นสิ่งที่ใช้ยืนยันตัวตน (authenticator) ตาม NIST ดังนั้น ชีวมิติต้องใช้เป็นส่วนหนึ่งของ Multi-factor authentication ร่วมกับสิ่งที่ใช้ยืนยันตัวตนประเภทสิ่งที่คุณมี (something you have) เท่านั้น